Visão geral

Introdução

O Citrix DaaS™ é um serviço que fornece virtualização de aplicativos e desktops, dando ao TI controle de máquinas virtuais, aplicativos e segurança hospedados no local ou na nuvem, ao mesmo tempo em que oferece acesso de qualquer lugar para qualquer dispositivo. Os usuários finais podem usar aplicativos e desktops independentemente do sistema operacional e da interface do dispositivo.

Usando o Citrix DaaS, você pode entregar aplicativos e desktops virtuais seguros para qualquer dispositivo, deixando a maior parte da instalação, configuração e atualizações para a Citrix. Você mantém controle total sobre aplicativos, políticas e usuários, ao mesmo tempo em que oferece a melhor experiência de usuário em qualquer dispositivo.

O Citrix DaaS permite que você gerencie cargas de trabalho de data center no local e de nuvem pública juntas em uma implantação híbrida. Você pode se conectar a nuvens públicas como Microsoft Azure, Amazon Web Services (AWS) e Google Cloud, além de hipervisores no local como XenServer®, Microsoft Hyper-V, Nutanix AHV e VMware vSphere. A abordagem híbrida e multi-nuvem oferece a flexibilidade de implantar diferentes aplicativos em diferentes locais de recursos em todo o mundo.

O Citrix DaaS oferece várias maneiras de entregar aplicativos e desktops.

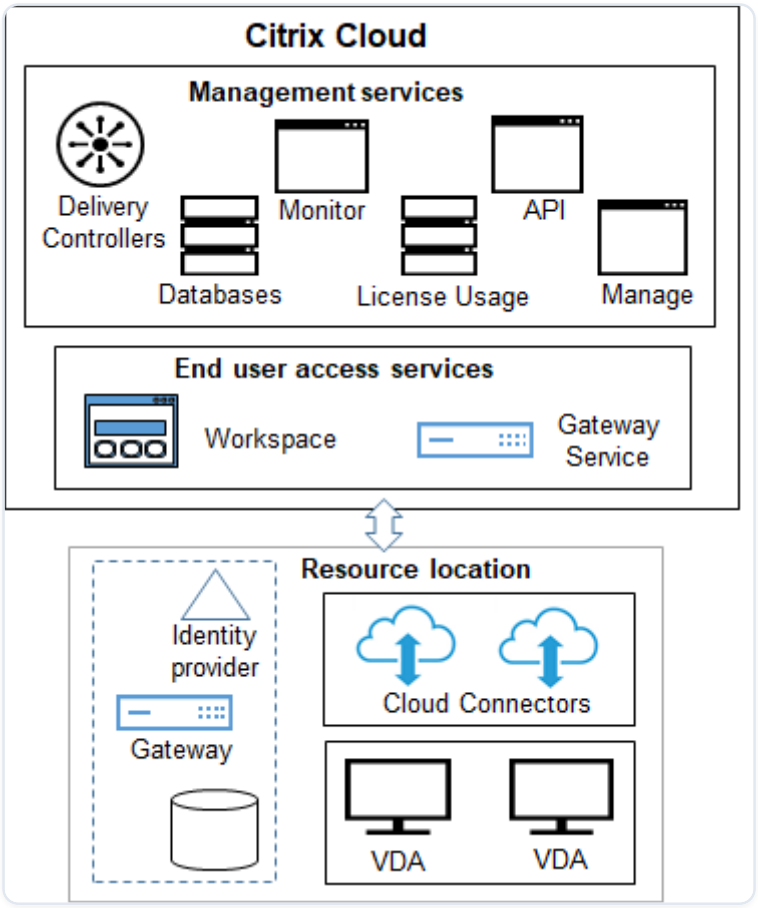
- Métodos de entrega descreve as principais formas, com casos de uso e prós/contras.
- Modelos de entrega lista mais opções e também oferece comparações de modelos VDI.

Citrix Managed Azure simplifica ainda mais a implantação de aplicativos e desktops virtuais. Com o Citrix Managed Azure, a Citrix também gerencia a hospedagem de cargas de trabalho do Azure.

Saiba mais sobre as vantagens de usar este serviço.

Visão geral do site

O gráfico a seguir mostra os serviços e componentes com os quais os administradores Citrix trabalham em uma implantação de produção do Citrix DaaS (também conhecida como site).



Conforme mostrado no gráfico, a Citrix gerencia os serviços e componentes de acesso e gerenciamento de usuários no Citrix Cloud. Os aplicativos e desktops que você entrega aos usuários residem em máquinas em um ou mais locais de recursos. Em uma implantação do Citrix DaaS, um local de recursos contém componentes da camada de acesso e das camadas de recursos. Cada local de recursos é considerado uma zona.

Se você migrou recentemente do Citrix Virtual Apps and Desktops™, verá que o Citrix DaaS elimina a maior parte do trabalho de configuração de componentes exigido em uma implantação no local.

Componentes e serviços gerenciados pela Citrix

- **Delivery Controllers:** O Citrix DaaS fornece a funcionalidade para balancear a carga de aplicativos e desktops, autenticar usuários e intermediar ou priorizar conexões diretamente da nuvem, sem a necessidade de gerenciar Delivery Controllers, como acontece com o Citrix Virtual Apps and Desktops.
- **Bancos de dados:** A configuração do site, o monitoramento e os dados de log de configuração são armazenados pelo serviço de nuvem, eliminando a necessidade de banco de dados SQL do produto Citrix Virtual Apps and Desktops local.
- **Licenciamento:** Gerencia licenças e fornece estatísticas de uso.

- **Studio:** Um console central baseado na web que permite configurar, gerenciar e monitorar suas implantações DaaS para fornecer aplicativos e desktops virtuais. Para obter mais informações, consulte Planejar e criar uma implantação e Gerenciar suas implantações.

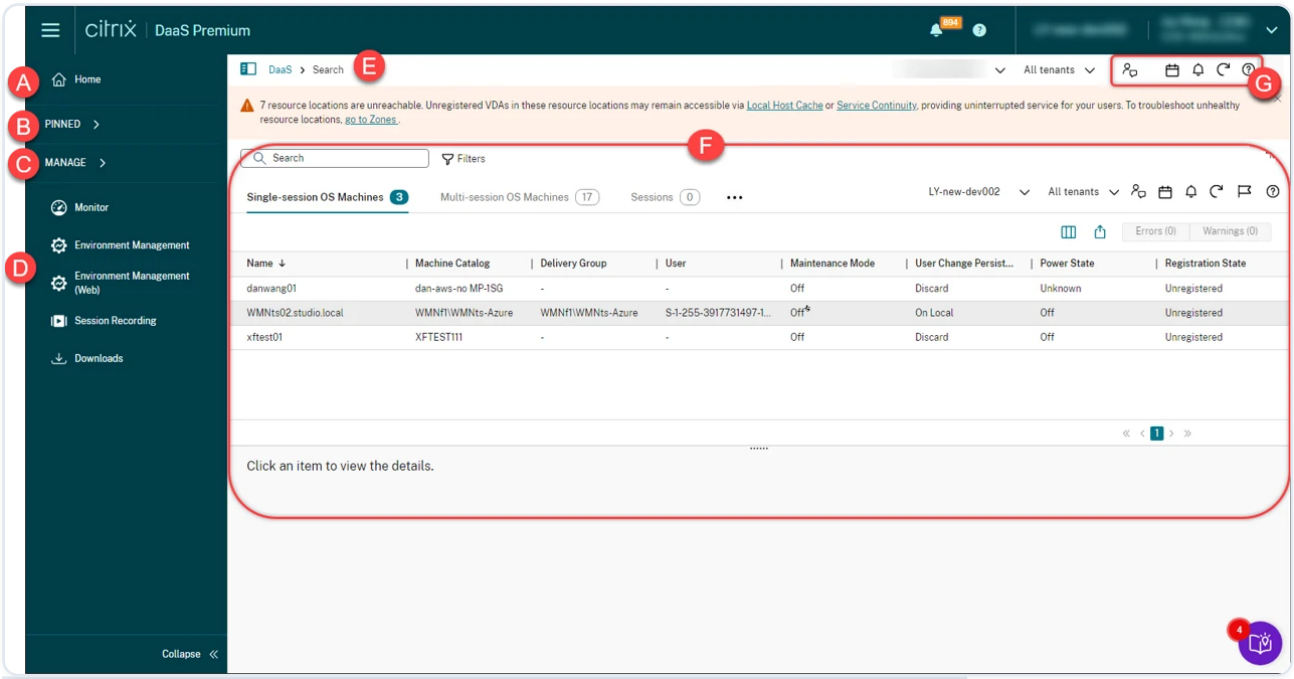
  Você também pode usar APIs de serviço e comandos PowerShell para configurar e gerenciar suas implantações DaaS.
- **Monitor:** O console Monitor permite que as equipes de suporte de TI e de help desk monitorem um ambiente, solucionem problemas antes que se tornem críticos e executem tarefas de suporte para usuários finais. As exibições incluem:
  - Dados de sessão em tempo real do Broker Service no Controller, que incluem dados do agente do broker no Virtual Deliver Agent (VDA).
  - Dados históricos do Monitor Service no Controller.
  - Dados sobre o tráfego HDX™ (também conhecido como tráfego ICA).
- **Cloud Connectors:** Um Cloud Connector é o canal de comunicação entre os componentes no Citrix Cloud e os componentes no local do recurso. No local do recurso, o Cloud Connector atua como um proxy para o Delivery Controller™ no Citrix Cloud.

  Cada local de recurso contém pelo menos um Cloud Connector. Dois ou mais Cloud Connectors são recomendados para redundância.
  - Ao usar o Studio para provisionar máquinas, você primeiro instala os Cloud Connectors a partir do console do Citrix Cloud™. Para obter detalhes, consulte Cloud Connectors.
  - Ao usar o Quick Deploy para provisionar máquinas Azure, a Citrix cria o local do recurso e os Cloud Connectors para você ao criar um catálogo.

  Após a instalação dos Cloud Connectors, a Citrix os gerencia e atualiza. As únicas tarefas tratadas pelo cliente são as atualizações do Windows e a aplicação de patches dos Cloud Connectors.

Studio

Studio é um portal central baseado na web que permite configurar, gerenciar e monitorar suas implantações DaaS para entregar aplicativos e desktops virtuais.



CHAMADA	ÁREA	DESCRIÇÃO
A	Início	Fornece uma visão geral da sua implantação e cargas de trabalho do Citrix DaaS, juntamente com informações que o ajudam a aproveitar ao máximo sua assinatura. Para obter mais informações, consulte a página Início.
B	FIXADO	Visível somente depois de fixar um nó no painel esquerdo. Lista os nós que você fixou.
C	GERENCIAR	• Nós relacionados à Configuração

CHAMADA	ÁREA	DESCRIÇÃO
		Completa: Permitem configurar e gerenciar suas implantações DaaS para entregar aplicativos e desktops virtuais. Os exemplos incluem: Pesquisa, Catálogos de Máquinas, Grupos de Entrega e muito mais. Para obter mais informações, consulte Planejar e construir uma implantação e Gerenciar implantações. • Nó de Implantação Rápida: Permite configurar e gerenciar rapidamente suas implantações DaaS

CHAMADA	ÁREA	DESCRIÇÃO	
		hospedadas por outros provedores de serviços em nuvem usando um fluxo de trabalho guiado. Escolha entre quatro provedores de hospedagem: Microsoft Azure, Microsoft Windows 365, Amazon WorkSpace Core e Google Cloud.	
D	Outros	• Nó de Monitoramento: Direciona você para a interface do Monitor. Para obter mais informações, consulte Monitor. • Nós de Serviço: Direciona você para as interfaces de serviços de valor agregado, como	

CHAMADA	ÁREA	DESCRIÇÃO
		Workspace Environment Management (web) service e Session Recording service. • Nó de Downloads: Direciona você para a página de Downloads, onde você pode baixar software para configurar e gerenciar seus recursos DaaS.
E	Trilha de navegação	Fornece contexto e permite uma navegação rápida de volta às páginas de nível superior.
F	Painel de trabalho	Exibe ações e detalhes de um nó selecionado.
G	Ações comuns	Exibe ações comuns como Enviar feedback, personalizar a página inicial, acessar a Central

CHAMADA	ÁREA	DESCRIÇÃO	
		de Notificações e muito mais. • A Central de Notificações fornece atualizações em tempo real e um histórico de 48 horas de operações de longa duração. Enquanto uma operação está em execução, uma notificação de status aparece abaixo da área de ações comuns para indicar seu progresso.	
		• O Centro de Tarefas exibe uma lista abrangente de todas as tarefas, organizadas por categoria. A interface do usuário fornece Filtro, Pesquisa e outros	

CHAMADA	ÁREA	DESCRIÇÃO
		controles consistentes com a visualização principal. Você pode executar ações em qualquer tarefa listada, incluindo ações comuns como **Excluir** e **Ver detalhes**, e ações específicas da tarefa, como Repetir tarefa e Exportar status da subtarefa.

Componentes e tecnologias gerenciados pelo cliente

- **Citrix Gateway:** Quando os usuários se conectam de fora do firewall corporativo, o Citrix DaaS pode usar a tecnologia Citrix Gateway para proteger essas conexões com TLS. O Citrix Gateway ou o appliance virtual VPX é um appliance SSL VPN implantado na DMZ. Ele fornece um único ponto de acesso seguro através do firewall corporativo.

  A Citrix instala e gerencia o serviço Citrix Gateway no Citrix Cloud. Você também pode, opcionalmente, instalar o Citrix Gateway em locais de recursos.

- **Active Directory:** O Active Directory é usado para autenticação e autorização. Ele autentica usuários e garante que eles estejam obtendo acesso aos recursos apropriados. A identidade de um assinante define os serviços aos quais ele tem acesso no Citrix Cloud. Essa identidade vem de contas de domínio do Active Directory fornecidas pelos domínios dentro do local do recurso.

- **Provedor de Identidade (IdP):** O IdP é a autoridade final para a identidade do usuário. Os IdPs suportados incluem: Active Directory local, Active Directory mais token, Microsoft Entra ID, Citrix Gateway e Okta. Para obter mais informações, consulte:
  - Resumo Técnico: Identidade do Workspace
  - Gerenciamento de identidade e acesso
- **Virtual Delivery Agents (VDAs):** Cada máquina física ou virtual que entrega recursos (aplicativos e desktops) deve ter um Citrix VDA instalado nela. Os VDAs estabelecem e gerenciam a conexão entre a máquina na qual está instalado e o dispositivo do usuário, e aplicam políticas configuradas para a sessão.

  O VDA se registra em um Delivery Controller, usando um Cloud Connector no local do recurso como proxy.

  Vários tipos de VDA estão disponíveis:

  - Os VDAs para sistemas operacionais Windows multi-sessão permitem que vários usuários se conectem à máquina ao mesmo tempo. Este tipo de VDA é geralmente instalado em servidores Windows.
  - Os VDAs para sistemas operacionais Windows de sessão única permitem que um usuário se conecte a uma máquina por vez. Este tipo de VDA é geralmente usado para VDI.

    Uma versão principal deste tipo de VDA está disponível para uso com o recurso Acesso Remoto a PC. Ela contém um subconjunto dos recursos do VDA de sessão única completo.
  - Os VDAs Linux suportam aplicativos e desktops virtuais baseados em uma distribuição RHEL, CentOS, SUSE ou Ubuntu.

  Ao longo da documentação deste serviço, “VDA” frequentemente se refere ao agente e à máquina na qual ele está instalado.
- **Hypervisores e serviços de nuvem:** Na maioria dos sites de produção, as instâncias de aplicativos e desktops (cargas de trabalho) que você disponibiliza (publica) para seus usuários são “hospedadas” por um hipervisor ou serviço de nuvem suportado. (O recurso Acesso Remoto a PC é geralmente usado com máquinas físicas. Portanto, ele não usa hipervisores ou serviços de nuvem para provisionamento de máquinas.)
  - Ao usar o Studio, você primeiro cria uma conexão com um hipervisor host ou serviço de nuvem suportado. Em seguida, você usa uma imagem (criada através desse host) para criar um catálogo de máquinas que contêm as instâncias de aplicativos e desktops.

Finalmente, você cria um grupo de entrega. A Citrix fornece várias ferramentas para simplificar e facilitar como esses hosts de sessão são construídos e mantidos.

- Ao usar o Quick Deploy para entregar cargas de trabalho do Azure, você só precisa criar o catálogo. Embora você possa usar sua própria assinatura do Azure ao criar o catálogo, usar uma assinatura Citrix Managed Azure elimina a necessidade de gerenciar o host também.

As instâncias de aplicativos e desktops que você publica podem ser locais, hospedadas em nuvens públicas ou em uma mistura híbrida de ambos.

- **Citrix StoreFront™:** Citrix StoreFront é a camada de acesso hospedada pelo cliente, como uma alternativa ao Citrix® StoreFront Cloud. Para obter mais informações, consulte StoreFront e Citrix® StoreFront Cloud).

Objetos que você configura para entregar desktops e aplicativos

Você configura os seguintes itens para entregar aplicativos e desktops em um ambiente de produção.

- **Conexão de host:** Uma conexão de host (mencionada anteriormente) ajuda a habilitar a comunicação entre os componentes no plano de controle (Citrix Cloud) e os VDAs em um local de recurso. As especificações de conexão incluem:

  - O endereço e as credenciais para acessar o host
  - O método de armazenamento a ser usado e as máquinas a serem usadas para armazenamento
  - Qual rede as VMs podem usar

  Lembre-se: Ao usar o Quick Deploy, você não precisa criar uma conexão. E se você usar Citrix Managed Azure, a Citrix também gerencia a hospedagem.

- **Catálogo:** Nas interfaces Studio e Monitor, os catálogos são chamados de “catálogos de máquinas”. Um catálogo é uma coleção de máquinas virtuais ou físicas que possuem o mesmo tipo de sistema operacional (por exemplo, Windows multi-sessão, Ubuntu single-session).

  Ao criar um catálogo, você geralmente usa uma imagem, que também é conhecida como modelo. (Os catálogos de Acesso Remoto a PCs geralmente contêm máquinas físicas, então nenhuma imagem é necessária.)

- Ao usar o Quick Deploy, a Citrix fornece várias imagens preparadas pela Citrix que você pode usar para criar suas próprias imagens personalizadas. Ou, você pode importar imagens de sua própria assinatura do Azure.
- Ao usar o Studio para criar VMs usando um tipo de host compatível, a imagem geralmente deve ser criada e residir em uma máquina host. Ao criar o catálogo, você fornece o caminho para essa imagem.

Independentemente de onde a imagem reside, você pode instalar aplicativos na imagem, se quiser que esses aplicativos estejam em todas as máquinas criadas a partir dessa imagem (e não quiser virtualizar esses aplicativos).

Depois que a imagem estiver pronta, você cria o catálogo.

- Para VMs, o MCS cria as máquinas e o catálogo.
- Para Acesso Remoto a PC, o MCS simplesmente cria o catálogo, porque as máquinas físicas já existem.

Para obter mais informações sobre o MCS, consulte Gerenciamento de imagens.

- **Grupo de entrega:** Um grupo de entrega especifica:
  - Uma ou mais máquinas de um catálogo.
  - Usuários que têm permissão para acessar essas máquinas.
  - Os aplicativos e desktops que os usuários podem acessar por meio de sua loja.

  Ao usar a Implantação Rápida, um grupo de entrega é criado automaticamente. (Ele aparece apenas na interface do Studio.)
- **Grupo de aplicativos:** Os grupos de aplicativos permitem gerenciar coleções de aplicativos. Você pode criar grupos de aplicativos para aplicativos compartilhados entre diferentes grupos de entrega ou usados por um subconjunto de usuários dentro de grupos de entrega. Os grupos de aplicativos são opcionais.

Azure Gerenciado pela Citrix

O Azure Gerenciado pela Citrix é uma opção disponível em várias edições do Citrix DaaS. O uso do Azure Gerenciado pela Citrix simplifica a implantação de aplicativos e desktops virtuais do Azure. A Citrix gerencia a infraestrutura para hospedar cargas de trabalho do Azure.

Com o Azure Gerenciado pela Citrix, você obtém uma assinatura do Azure gerenciada pela Citrix e um local de recurso dedicados. Nessa assinatura do Azure, você cria um catálogo de VMs. Você pode:

- Implantar máquinas Windows OS de sessão única e multi-sessão ou máquinas Linux OS, de várias versões suportadas.
- Escolher em uma lista selecionada de tipos de computação e opções de armazenamento em regiões selecionadas.
- Provisionar cargas de trabalho persistentes ou não persistentes nessas máquinas.
- Escolha entre várias imagens fornecidas pela Citrix que têm o VDA mais recente instalado. Em seguida, a partir da interface Citrix, você cria sua própria imagem a partir desse modelo e a personaliza. Você também pode importar e usar imagens de suas próprias assinaturas do Azure.

Embora a Citrix gerencie a capacidade do Azure, se você quiser se comunicar com recursos existentes em sua própria assinatura do Azure, poderá usar o emparelhamento de VNet do Azure para conectar recursos. Você também pode usar o gateway VPN do Azure para se conectar diretamente aos seus recursos locais.

Para obter informações sobre segurança e responsabilidades ao usar o Citrix Managed Azure, consulte Visão geral de segurança técnica para Citrix Managed Azure.

Como solicitar o Citrix Managed Azure

Para obter uma assinatura do Citrix Managed Azure, você deve assinar uma oferta de serviço Citrix compatível e, em seguida, solicitar Fundos de Consumo do Citrix Managed Azure. Você pode solicitar o Citrix DaaS e os fundos de consumo através da Citrix ou do Azure Marketplace. O Citrix Managed Azure é compatível com as seguintes ofertas de serviço:

- Edições Citrix DaaS, Advanced, Advanced Plus e Premium
- Edição Citrix DaaS Standard para Azure

Para obter detalhes, consulte Inscrever-se no Citrix DaaS.

Resumo dos benefícios do Citrix Managed Azure

O uso do Citrix Managed Azure oferece vários benefícios:

- Caminho mais rápido para benefícios de nuvem híbrida.

- Descarrega o gerenciamento de infraestrutura de TI. Oferece uma experiência de administração que coloca a TI no controle sem os desafios de gerenciamento e manutenção.
- Permite escalar rapidamente as soluções de trabalho.
- Fornece uma assinatura separada do Azure que é gerenciada e mantida pela Citrix. Isso isola a atividade de suas outras assinaturas do Azure.
- Você mantém a flexibilidade para criar e gerenciar cargas de trabalho usando suas próprias assinaturas do Azure. Sua implantação pode incluir cargas de trabalho que usam a assinatura do Citrix Managed Azure e cargas de trabalho que usam suas próprias assinaturas do Azure (gerenciadas pelo cliente).
- Usa um modelo de Infraestrutura como Serviço (IaaS) baseado em consumo real.
- Várias tecnologias estão disponíveis para criar conexões com suas próprias redes locais (como emparelhamento de VNet do Azure e gateway VPN do Azure). Isso permite que seus usuários acessem os recursos da sua rede, como servidores de arquivos.

A implantação e o gerenciamento do Citrix Managed Azure a partir deste serviço usam a interface de gerenciamento Quick Deploy.

Para obter mais informações, entre em contato com seu representante Citrix.

Entrega de aplicativos e desktops aos usuários

Citrix® StoreFront e Citrix® StoreFront Cloud

StoreFront e Citrix® StoreFront Cloud são as camadas de acesso, fornecendo uma interface de usuário para que os usuários finais visualizem e iniciem aplicativos e desktops. Dentro do StoreFront e do Citrix® StoreFront Cloud, você pode definir uma ou mais lojas, cada uma com uma URL. Os usuários finais podem acessar essas lojas usando o aplicativo Citrix Workspace ou um navegador da web.

- Citrix® StoreFront Cloud é a camada de acesso gerenciada pela Citrix. Depois de provisionar o DaaS, o **Citrix® StoreFront Cloud** estará disponível no menu principal. Você deve configurar a URL, a autenticação e outras configurações. Para obter mais informações, consulte Introdução ao Citrix® StoreFront Cloud.
- StoreFront é a camada de acesso gerenciada pelo cliente. Você pode instalar o StoreFront em servidores na sua rede corporativa. Os usuários finais podem se conectar diretamente às lojas hospedadas pelo StoreFront pela rede. Você pode fornecer acesso remoto usando um Citrix Gateway. O StoreFront pode usar o Local Host Cache para fornecer acesso a recursos quando o DaaS não estiver acessível. Para obter mais informações, consulte Introdução.

Consulte Acesso do usuário para considerações sobre o uso do StoreFront em um ambiente de serviço.

Você pode usar ambas as camadas de acesso. Por exemplo, você pode usar o Citrix® StoreFront Cloud para acesso remoto, enquanto implanta o StoreFront local para áreas da sua rede corporativa que precisam de maior resiliência contra interrupções de rede.

Aplicativo Citrix Workspace

Do lado do usuário, o aplicativo Citrix Workspace é instalado em dispositivos de usuário e outros endpoints, como desktops virtuais. O aplicativo Citrix Workspace fornece aos usuários acesso seguro e de autoatendimento a documentos, aplicativos e desktops de qualquer dispositivo, incluindo smartphones, tablets e PCs. O aplicativo Citrix Workspace fornece acesso sob demanda a aplicativos Windows, web e Software como Serviço (SaaS).

Para dispositivos que não podem instalar o software do aplicativo Citrix Workspace, o aplicativo Citrix Workspace para HTML5 fornece uma conexão através de um navegador da web compatível com HTML5.

O aplicativo Citrix Workspace está disponível para vários sistemas operacionais. Para obter detalhes, consulte Aplicativo Citrix Workspace.

Acordo de Nível de Serviço

O Citrix DaaS é projetado usando as melhores práticas da indústria para alcançar escala de nuvem e um alto grau de disponibilidade de serviço.

Para detalhes completos sobre o compromisso da Citrix com a disponibilidade dos serviços Citrix Cloud, consulte o Contrato de Nível de Serviço.

O desempenho em relação a essa meta pode ser monitorado continuamente em `<https://status.cloud.com>`.

Limitações

O cálculo desta Meta de Nível de Serviço não incluirá a perda de disponibilidade pelas seguintes causas:

- Falha do cliente em seguir os requisitos de configuração para o Citrix DaaS documentados na documentação do produto em `<https://docs.citrix.com>`.

- Causado por qualquer componente não gerenciado pela Citrix, incluindo, mas não se limitando a, máquinas físicas e virtuais controladas pelo cliente, sistemas operacionais instalados e mantidos pelo cliente, equipamentos de rede ou outro hardware instalados e controlados pelo cliente; configurações de segurança, políticas de grupo e outras políticas de configuração definidas e controladas pelo cliente; falhas de provedores de nuvem pública, falhas de Provedores de Serviços de Internet ou outros fatores externos ao controle da Citrix.
- Interrupção do serviço devido a razões além do controle da Citrix, incluindo desastres naturais, guerra ou atos de terrorismo, ação governamental.

Mais informações

- Diagramas do Citrix DaaS
- Arquitetura de Referência e Métodos de Implantação do Citrix DaaS
- Visão geral de segurança técnica
- Portas de rede
- Avisos de terceiros
- Requisitos do sistema
- Recursos
  - Uma introdução às (/pt-br/citrix-daas/hdx-transport.html) tecnologias HDX, além de detalhes sobre (/pt-br/citrix-daas/devices.html) Dispositivos, (/pt-br/citrix-daas/graphics.html) Gráficos e (/pt-br/citrix-daas/multimedia.html) Multimídia.
  - (/pt-br/citrix-daas/install-configure/remote-pc-access.html) Acesso Remoto a PC: Permite que os usuários façam logon remotamente de qualquer lugar em um PC físico no escritório. Você pode configurar o Acesso Remoto a PC usando o Studio.
  - (/pt-br/citrix-virtual-apps-desktops/install-configure/publish-content.html) Publicar conteúdo: Publique um aplicativo que seja simplesmente um URL ou um caminho UNC para um recurso.
  - (/pt-br/citrix-virtual-apps-desktops/install-configure/server-vdi.html) VDI de Servidor: Forneça um desktop a partir de um sistema operacional de servidor para um único usuário.
- Para Citrix DaaS Standard para Azure, consulte (/pt-br/citrix-daas-azure) sua documentação de produto dedicada.
- Para saber mais sobre a disponibilidade de recursos nos produtos e edições do Citrix DaaS, consulte a matriz de recursos do Citrix DaaS.

- A Série de Aprendizagem do Citrix Cloud oferece um curso de treinamento para você começar a usar o Citrix Cloud e seus serviços. Você pode visualizar sequencialmente todos os módulos, desde introduções até o planejamento e a construção de serviços. Você também pode escolher módulos individuais ou segmentos específicos de tarefas dentro de um módulo. Consulte Série de Aprendizagem do Cloud.

Começar

Para saber como configurar sua implantação, comece com (/pt-br/citrix-daas/install-configure.html) Planejar e construir uma implantação. Esse resumo o guia pelas principais etapas do processo e fornece links para mais informações e procedimentos detalhados.

Novidades

Um objetivo da Citrix® é entregar novos recursos e atualizações de produtos aos clientes do Citrix DaaS™ assim que estiverem disponíveis. Novas versões oferecem mais valor, então não há razão para atrasar as atualizações. As atualizações contínuas para o Citrix DaaS são lançadas aproximadamente a cada três semanas.

Este processo é transparente para você. As atualizações iniciais são aplicadas apenas aos sites internos da Citrix e, em seguida, são aplicadas gradualmente aos ambientes dos clientes. Entregar atualizações incrementalmente em ondas ajuda a garantir a qualidade do produto e maximizar a disponibilidade.

É possível que as atualizações mencionadas nesta documentação estejam sendo implementadas e não estejam acessíveis a todos os clientes ao mesmo tempo.

Para obter detalhes sobre o Acordo de Nível de Serviço para escala de nuvem e disponibilidade de serviço, consulte Acordo de Nível de Serviço. Para monitorar interrupções de serviço e manutenção programada, consulte o Painel de Integridade do Serviço.

Use estes artigos para saber mais sobre atualizações de versão, problemas conhecidos, descontinuações e remoções, e recursos em pré-visualização:

- Novidades lista recursos novos e aprimorados nas versões recentes.
- Problemas conhecidos lista problemas que podem afetar as implantações.
- Descontinuações e remoções fornece aviso prévio sobre recursos que foram descontinuados, removidos ou planejados para remoção.
- Recursos em pré-visualização lista recursos de pré-visualização disponíveis para ambientes de não produção ou produção limitada e oferece uma forma de enviar feedback.

O que há de novo

Este artigo lista os recursos novos e aprimorados do Citrix DaaS™. As atualizações são organizadas por mês de lançamento.

Virtual Delivery Agents (VDAs)

Os VDAs para máquinas Windows geralmente são lançados ao mesmo tempo que o produto Citrix Virtual Apps and Desktops™.

- Para obter informações sobre os novos recursos de VDA e HDX, consulte os artigos O que há de novo e Problemas conhecidos para a versão atual do Citrix Virtual Apps and Desktops.
- Para obter informações sobre plataformas VDA e recursos que não são mais suportados, consulte Descontinuação. Esse artigo também inclui plataformas e recursos que não serão suportados em uma versão futura (como quais sistemas operacionais suportam a instalação do VDA).

> **Importante:**
>
> Se o componente Personal vDisk (PvD) foi instalado em um VDA, esse VDA não pode ser atualizado para a versão 1912 LTSR ou posterior. Para usar o novo VDA, você deve desinstalar o VDA atual e, em seguida, instalar o novo VDA. (Esta instrução se aplica mesmo se você instalou o PvD, mas nunca o usou.) Para obter detalhes, consulte Se o VDA tiver o Personal vDisk instalado.

Agosto de 2026

Recursos novos e aprimorados

Limiares. O Monitor agora oferece suporte a limiares configuráveis para métricas do sistema. Defina os estados Crítico, Aviso e Saudável para métricas como uso da CPU, uso da memória, ICA RTT, latência da rede e duração do logon em fontes de dados, incluindo Máquinas, Sessões, Cloud Connectors, Provisioning Services e StoreFront. Indicadores codificados por cores aparecem nas páginas Painel, Infraestrutura, Filtros e Detalhes do Usuário/Máquina. Crie limiares personalizados para cargas de trabalho específicas ou use limiares predefinidos com padrões dinâmicos que se adaptam automaticamente ao seu ambiente.

Para obter mais informações, consulte Limiares

Citrix Advisor: Execuções agendadas e widget da página inicial. O Advisor agora executa verificações de site automaticamente em um agendamento semanal recorrente. Cada execução gera um relatório retido por até 90 dias.

Além disso, um novo widget **Advisor** na página **Início** exibe um resumo de recomendações agrupadas por nível de impacto e filtráveis por categoria, para que você possa identificar e agir rapidamente sobre itens críticos.

Para obter mais informações, consulte Verificar recomendações e Widget do Advisor.

Logon único do Microsoft Entra. A partir da versão 2607 do VDA, você pode usar a configuração de política de máquina de logon único do Microsoft Entra para habilitar ou desabilitar esse recurso em seus hosts de sessão.

Logon web (Pré-visualização). Você pode habilitar o logon baseado na web para fazer login ou desbloquear seu desktop virtual unido ao Entra ou unido ao Entra híbrido. Consulte Logon web para obter detalhes.

Latência do Connector Appliance para o aplicativo de backend na Topologia de Aplicativos. A Topologia de Aplicativos do Secure Private Access agora mostra um valor de **Latência de Conexão** no link entre o Connector Appliance e o aplicativo de backend, completando a visualização de latência hop-by-hop. O valor é um tempo de ida e volta sintético P90 que o Connector Appliance mede na última hora. Atualmente, isso abrange implantações em nuvem.

Para obter mais informações, consulte Latência do Connector Appliance para o aplicativo de backend.

Julho de 2026

Novos recursos e aprimoramentos

Aprimoramentos na experiência do catálogo de máquinas no Studio. Aprimoramos a experiência do catálogo de máquinas no Studio exibindo o esquema de nomenclatura configurado nos detalhes do catálogo de máquinas e otimizando a barra de ações com base na frequência de uso. **Visualizar Máquinas** agora é uma ação de nível superior, enquanto **Excluir Catálogo de Máquinas** foi movido para o menu **Mais** devido ao seu uso infrequente.

Para obter mais informações, consulte Gerenciar catálogos de máquinas.

Citrix Advisor: Novas verificações para confiabilidade, desempenho e excelência operacional. O Citrix Advisor agora inclui as seguintes novas verificações de ambiente que fornecem recomendações acionáveis para ajudar a melhorar a confiabilidade, o desempenho e a excelência operacional:

- Confiabilidade

    - Verificar a comunicação do Cloud Connector com o StoreFront
- Desempenho
    - Colocar servidores StoreFront em uma rede de baixa latência
- Excelência operacional
    - Revisar máquinas em modo de manutenção por períodos prolongados
    - Reduza o tempo de solução de problemas com o Always On Tracing

Esses aprimoramentos ajudam você a identificar proativamente problemas e tomar ações corretivas. Para obter mais informações, consulte Citrix Advisor.

Estenda a pesquisa de log de configuração para incluir detalhes de operação de baixo nível. Agora você pode estender o escopo da pesquisa na seção **Logging** do **Web Studio** para incluir detalhes de operação de baixo nível. Ao selecionar **Extend search scope to include details**, você pode pesquisar detalhes de baixo nível, como nome da máquina, nome VDI e assim por diante.

Para obter mais informações, consulte Exibir conteúdo do log de configuração.

Exclua máquinas em drenagem do buffer de capacidade do Autoscale. Agora você pode excluir máquinas que estão em drenagem devido a reinicializações agendadas do cálculo do buffer de capacidade do Autoscale para grupos de entrega de SO de várias sessões. Quando esta opção está ativada, apenas as máquinas que estão totalmente disponíveis para aceitar novas sessões são contadas ao determinar a capacidade necessária. Isso ajuda a evitar o superprovisionamento que pode ocorrer quando as máquinas em drenagem são incluídas no buffer.

Para obter mais informações sobre como configurar a opção usando o Web Studio, consulte Configurações baseadas em agendamento e baseadas em carga.

Alternativamente, para configurar usando o PowerShell, consulte Excluir máquinas em drenagem dos cálculos de autoscale.

Links diretos do Citrix Aidrien para o DaaS. Quando você pergunta ao Citrix Aidrien sobre máquinas ou sessões, as respostas agora incluem links diretos para a visualização correspondente do console DaaS com filtros de pesquisa aplicados automaticamente. Isso permite que você pule diretamente de uma resposta de chat para a interface relevante sem navegar manualmente ou reconstruir filtros.

Suporte a escopo para zonas. Agora você pode aplicar controle de escopo a zonas (conhecidas como locais de recurso no Citrix Cloud). Este aprimoramento estende os recursos de controle de escopo existentes no Citrix DaaS para os objetos de zona, permitindo que você conceda a administradores personalizados acesso com escopo a zonas específicas. Com este suporte, você pode alinhar o acesso administrativo mais de perto com os requisitos operacionais e de segurança da sua organização. Para obter mais informações, consulte Atribuir escopos a uma zona.

Configure o BYOL separadamente após conectar sua conta AWS. Agora você pode conectar uma conta do Amazon Web Services (AWS) ao Web Studio sem configurar o suporte a Bring Your Own License (BYOL) durante o processo de conexão da conta. Anteriormente, a configuração do BYOL era uma etapa obrigatória no assistente **Connect AWS account** ao conectar-se a uma região habilitada para BYOL. Agora você pode conectar sua conta primeiro e, em seguida, configurar o suporte a BYOL a qualquer momento, selecionando **Set up BYOL** na lista **Accounts** ou no painel de detalhes da conta. O assistente **Set up BYOL** o guia pela habilitação do BYOL no console do AWS WorkSpaces e pela importação de uma imagem de desktop do Windows 10 ou 11 para sua implantação do Citrix on Amazon WorkSpaces Core.

Para obter mais informações, consulte Configurar BYOL para sua conta.

Seleção de domínio mais rápida com pesquisa. Encontrar domínios do Active Directory e unidades organizacionais (OUs) agora é mais rápido no Web Studio. Durante a criação do catálogo de máquinas, ao selecionar **Create new Active Directory accounts**, você pode pesquisar um domínio específico diretamente na lista suspensa **Location (domain)** em vez de navegar pela lista completa de domínios confiáveis.

Para obter mais informações, consulte Pool de identidades de identidade de máquina unida ao Active Directory local.

Task Center: Guia Recorrente e gerenciamento de tarefas aprimorado. O Task Center agora inclui uma guia **Recurring** que mostra as tarefas agendadas para serem executadas periodicamente ou no futuro. Além da guia **Recent tasks** existente, que mostra execuções de tarefas individuais dos últimos 90 dias, agora você pode:

- Pesquisar e filtrar tarefas recentes e recorrentes.
- Acompanhe o status da tarefa em tempo real e o estado do agendamento recorrente.
- Execute ações em tarefas recentes, como cancelar ou executar novamente.
- Execute ações em agendamentos recorrentes, como editar ou excluir.

Para obter mais informações, consulte Monitorar e gerenciar tarefas no Centro de Tarefas.

Restringir atualizações de VDA a máquinas marcadas. Agora você pode limitar as atualizações de VDA em nível de catálogo a um subconjunto específico de máquinas usando tags de máquina no Web Studio. Ao agendar uma atualização, selecione **Atualizar máquinas que correspondem à tag**, escolha uma tag, e somente as máquinas com essa tag serão incluídas.

Isso ajuda a suportar estratégias de atualização baseadas em anel, onde os administradores validam uma nova versão do VDA com um grupo piloto antes de implementá-la para todo o catálogo.

Para obter mais informações, consulte Atualizar VDAs usando VUS.

Selecione as regiões de replicação do Azure ao criar uma versão de imagem. O Studio agora inclui uma página **Compartilhamento de Imagem** durante a criação da versão da imagem, onde você pode selecionar uma ou mais regiões do Azure para replicar automaticamente a imagem preparada. Você pode selecionar recursos de diferentes conexões de hospedagem e, opcionalmente, atribuir uma chave de criptografia de disco regional. Esta página aparece somente quando **Armazenar versões de imagem na Galeria de Computação do Azure** está habilitado na definição da imagem. Para obter mais informações, consulte Criar versões de imagem.

Junho de 2026

Novos recursos e aprimoramentos

Acesse dados do Citrix DaaS no Aidrien. O Aidrien pode recuperar e exibir dados do ambiente Citrix DaaS diretamente no chat, permitindo que você investigue problemas e gerencie recursos sem sair da conversa. Usando linguagem natural, você pode pesquisar e visualizar informações sobre:

- Máquinas e sessões
- Catálogos de máquinas
- Grupos de entrega

O Aidrien apresenta os dados recuperados diretamente na interface do usuário do chat, facilitando a exploração do seu ambiente, a identificação de problemas e a coleta de informações durante os fluxos de trabalho de solução de problemas.

Para obter mais informações, consulte Access Citrix DaaS data in Aidrien.

Relatórios de proteção de aplicativos no Citrix Monitor. Relatórios em tempo real de ativações de políticas de proteção e detecções de risco de segurança estão disponíveis no Citrix Director e Monitor. Os relatórios permitem que você avalie rapidamente o risco e configure suas políticas de

proteção para garantir um ambiente mais seguro. Através do gerenciamento proativo de riscos e da reconfiguração de políticas, você pode fortalecer a segurança do endpoint em seu ambiente e reduzir a exposição a ameaças emergentes. Para obter mais informações, consulte Endpoint Security policy activation & threat detection reporting

Tipos de armazenamento SSD do Azure para discos de SO efêmeros. O Studio agora permite que os Catálogos de Máquinas do Azure que usam Discos de SO Efêmeros do Azure selecionem o tipo de armazenamento de disco gerenciado do SO base (Premium SSD, Standard SSD ou Standard HDD) durante a criação do catálogo e as atualizações subsequentes de catálogo/esquema, com validação de UI e verificações pré-voo para evitar configurações não suportadas. Para obter mais informações, consulte Use Azure ephemeral OS disk.

Visibilidade da versão do SO do endpoint. Agora você pode gerenciar e rastrear sessões e conexões de usuário de forma mais eficaz por meio de aprimoramentos nas páginas de Sessão e Conexão. Essas páginas agora incluem uma coluna de Versão do SO do Endpoint e um filtro correspondente para dispositivos Windows e Linux.

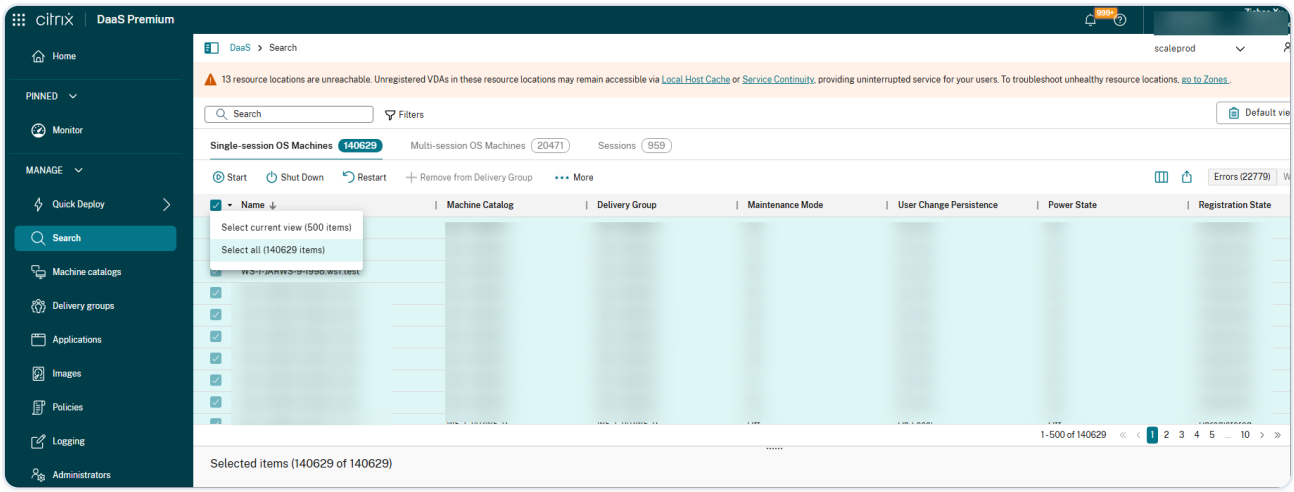
Isso ajuda você a:

- Visualizar a versão do sistema operacional do endpoint diretamente nas páginas de Sessão e Conexão.
- Filtrar sessões ou conexões com base em versões específicas do sistema operacional Windows ou Linux.

Para obter mais informações, consulte Endpoint OS Version Visibility

Ações em massa aprimoradas no Web Studio. Agora você pode selecionar todos os itens em todas as páginas ou apenas dentro da página atual. Este aprimoramento remove o limite anterior de 500 itens para operações em massa em resultados de pesquisa correspondentes, melhorando a eficiência administrativa em grandes ambientes com milhares de VDAs ou sessões.

Otimizações de desempenho também foram implementadas para garantir que as ações em massa permaneçam suaves e responsivas em escala.



Visualização de topologia expandida para Chrome Enterprise Premium e qualidade de dados de avaliação de políticas aprimorada. O Citrix Monitor agora mostra seis variantes de topologia do Chrome Enterprise Premium abrangendo implantações em nuvem e híbridas em rotas de aplicativos internas, externas e externas de IP fixo. O painel **Policy Evaluation** também pode transportar os valores de **Application Name**, **Application Type**, **Policies** e **Security Controls** de eventos de enumeração quando um evento de inicialização de aplicativo os omite; o campo **Data path** pode aparecer vazio quando o evento de origem não o especifica.

Para obter mais informações, consulte Chrome Enterprise Premium topology variants.

Suporte ao gerenciamento de imagens: pesquisa de imagens preparadas

Agora você pode usar uma barra de pesquisa no nó **Imagens** para filtrar e encontrar versões de imagem por critérios como nome da definição da imagem, número da versão da imagem, descrição da versão da imagem, tipo de SO, tipo de hypervisor, nome da conexão do host, nome da unidade do host, tipo de conexão do host, nome da imagem mestre, contagem do esquema de provisionamento e hora de criação da versão. Este aprimoramento ajuda os administradores a gerenciar eficientemente as imagens em grandes implantações.

Para mais informações, consulte Gerenciamento de imagens.

Suporte para criação de catálogos do Citrix Provisioning em ambientes de virtualização OpenShift usando o Studio

Com o Studio, agora você pode criar catálogos do Citrix Provisioning em ambientes de virtualização OpenShift. Anteriormente, você precisava alternar entre diferentes consoles para provisionar e gerenciar esses catálogos. Esse recurso simplifica o processo, permitindo que você execute tarefas de provisionamento e gerenciamento de energia inteiramente dentro do Studio.

Para mais informações, consulte Criar catálogos do Citrix Provisioning™ no Citrix Studio.

Suporte para criação de catálogos do Citrix Provisioning no Citrix Web Studio para Nutanix AHV Prism Central

Agora você pode criar um catálogo do Citrix Provisioning usando o Web Studio com o tipo de conexão de host Nutanix AHV Prism Central.

Esta implementação oferece as seguintes vantagens:

- Um único console para gerenciar catálogos MCS e Citrix Provisioning.
- Novos recursos para catálogos do Citrix Provisioning, como gerenciamento de identidade.

Para mais informações, consulte Criar catálogos do Citrix Provisioning™ no Citrix Studio.

Maio de 2026

Recursos novos e aprimorados

Suporte do Studio para controlar a visibilidade de aplicativos empacotados. Com o Studio, agora você pode controlar a visibilidade de um aplicativo empacotado — em um desktop, em **Citrix Workspace > Aplicativos**, ou em ambos. Para alterar a visibilidade de um aplicativo empacotado específico, vá para o nó **Aplicativos**, selecione o aplicativo e escolha **Propriedades > Entrega**.

Por padrão, os aplicativos empacotados são entregues apenas em **Citrix Workspace > Aplicativos**. Para mais informações, consulte Alterar propriedades do aplicativo.

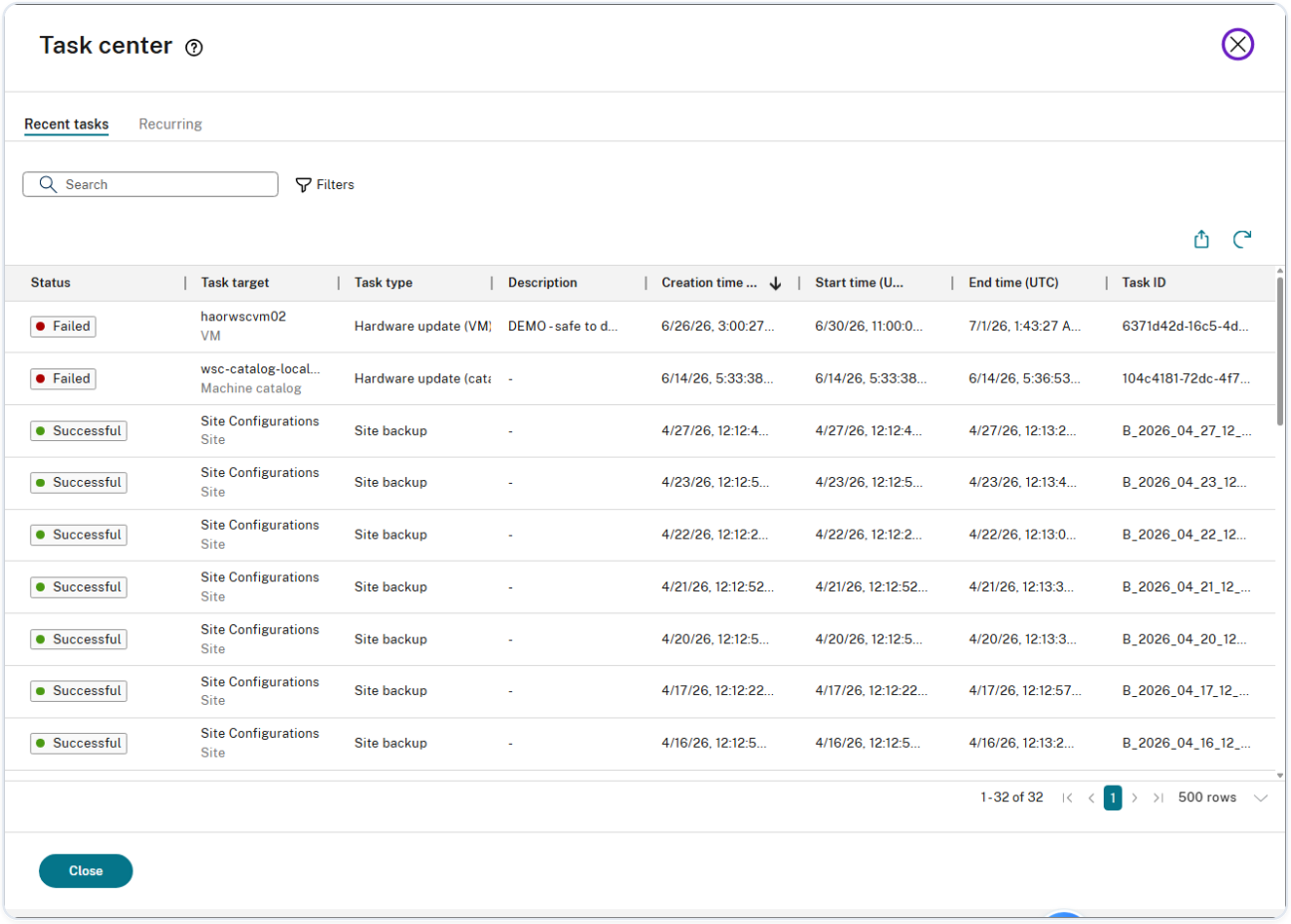
Capacidade de ver sessões e pontuação de componentes e correlacionar com o desempenho da sessão. A visão geral da experiência da sessão agora está disponível no painel Monitor. O resumo da experiência fornece insights sobre o número de sessões analisadas em um determinado período e a categorização das sessões analisadas em Boa, Média e Ruim. A categorização da sessão é feita com base nas pontuações da sessão. Para uma visão rápida da saúde geral do ambiente, o resumo também inclui a pontuação média da sessão e a pontuação média do componente das sessões analisadas. A pontuação do componente pode ser utilizada para solucionar problemas de desempenho da sessão, pois fornece uma camada adicional de detalhes para a análise. Para mais informações, consulte Pontuação da Sessão

Suporte para aplicativos Numecent Cloudpaging. Agora você pode descobrir e publicar aplicativos Numecent Cloudpaging usando o nó **Pacotes de aplicativos** no Web Studio. Você também pode armazenar contêineres de aplicativos Numecent Cloudpaging em um compartilhamento de arquivos de rede de sua escolha e descobri-los e entregá-los aos usuários finais no Studio, especificando o caminho do compartilhamento de arquivos. Essa capacidade

simplifica a descoberta de aplicativos e expande suas opções para se afastar da infraestrutura App-V. Para obter mais informações, consulte Aplicativos Cloudpaging.

Central de Tarefas agora disponível. A Central de Tarefas fornece uma visão centralizada das tarefas agendadas e recorrentes no Studio, ajudando você a rastrear os seguintes status de tarefa: Agendada, Concluída, Falha ou Prestes a ser executada. Você pode acessar a Central de Tarefas selecionando o ícone de calendário no canto superior direito do console do Studio.

Para obter mais informações, consulte Monitorar e gerenciar tarefas na Central de Tarefas.



Filtragem de recursos. O recurso de filtragem de recursos permite configurar regras para controlar o acesso do usuário a recursos em grupos de entrega. Você pode definir o tipo de recurso (aplicativo, desktop ou ambos), aplicar restrições de tag e definir condições para a aplicação de regras com base em fatores como localização da rede e contexto de conexão da loja. Para acessar o recurso, vá para **Grupos de entrega > Configurações > Filtro de recursos**. Para obter mais informações, consulte Restringir o acesso do usuário a recursos em todos os grupos de entrega.

Instâncias Gerenciadas do Amazon WorkSpaces Core: Suporte do Studio para cache de write-back de E/S do MCS (MCSIO). Agora você pode configurar as configurações de cache de write-back (WBC) da Otimização de Armazenamento do MCS (MCSIO) diretamente no Citrix

Studio ao criar ou editar catálogos de máquinas para Instâncias Gerenciadas do Amazon WorkSpaces Core. Anteriormente, a configuração do cache de write-back estava disponível apenas por meio de comandos do PowerShell. O Studio agora expõe as opções de cache de write-back na página Configurações de Disco do assistente de Configuração de Catálogo de Máquinas, incluindo tamanho do disco de cache, alocação de memória, tipo de armazenamento EBS (por exemplo, gp2, gp3, io1, io2), persistência do disco em ciclos de energia e retenção do disco do SO para tempos de inicialização mais rápidos. Para obter mais informações, consulte Catálogo habilitado para MCSIO.

Abril de 2026

Recursos novos e aprimorados

Logon único do Microsoft Entra. A opção **Desconectar sessão remota ao bloquear para autenticação da plataforma de identidade da Microsoft** agora é compatível com o VDA de sessão única. Consulte comportamento de bloqueio de sessão para obter detalhes.

Atualizar discos BDM para catálogos do Citrix Provisioning. Agora você pode atualizar discos BDM (Boot Device Management) para seus catálogos do Citrix Provisioning provisionados pelo MCS (Machine Creation Services). A atualização do disco BDM ajuda a atualizar os endereços do servidor Citrix Provisioning e o firmware UEFI usando o Studio ou o PowerShell. Esse recurso economiza esforço administrativo e mantém seu ambiente atualizado. Ele simplifica o gerenciamento de catálogos sem recriar máquinas virtuais. Ele oferece suporte a ambientes Azure, Nutanix AHV Prism Central, VMware e XenServer. Para obter mais informações, consulte Atualizar discos BDM.

Atualizar atribuições de vDisk para catálogos do Citrix Provisioning provisionados por MCS. Agora você pode atualizar as atribuições de vDisk para catálogos do Citrix Provisioning provisionados por MCS existentes usando o Studio ou o PowerShell. Anteriormente, você precisava recriar catálogos para alterar vDisks. Esse aprimoramento economiza tempo e esforço, permitindo que você gerencie as atribuições. Você pode listar os vDisks disponíveis e atribuir vDisks existentes no nível do catálogo. Esse recurso se aplica a ambientes Azure, Nutanix AHV Prism Central, VMware e XenServer. Observe que o gerenciamento do ciclo de vida do vDisk permanece dentro do console do Citrix Provisioning. Para obter mais informações, consulte Atualizar atribuição de vDisk.

Redefinir disco do SO para VMs persistentes no Nutanix AHV Prism Central. Com esse recurso, agora você pode redefinir o disco do SO para VMs persistentes usando o comando

PowerShell `Reset-ProvVMDisk` em ambientes Nutanix AHV Prism Central. Para obter mais informações, consulte Redefinir disco do SO para VMs persistentes.

Citrix Advisor: Novas verificações de segurança, confiabilidade, desempenho e excelência operacional. O Citrix Advisor agora inclui as seguintes novas verificações de ambiente que fornecem recomendações acionáveis para ajudar a melhorar a segurança, confiabilidade, desempenho e excelência operacional para StoreFront, VDAs e Active Directory:

- Segurança
  - Corrigir vulnerabilidades de segurança do VDA
  - Resolver vulnerabilidades de segurança do aplicativo Citrix Workspace
  - Atualizar versões do servidor StoreFront que atingiram o Fim da Vida Útil
  - Usar HTTPS para a URL base do StoreFront
  - Usar HTTPS para comunicação entre StoreFront e Cloud Connectors
  - Revisar lojas StoreFront com acesso anônimo habilitado
- Confiabilidade
  - Garantir redundância do servidor StoreFront
- Desempenho
  - Habilitar pool de sockets para lojas StoreFront
- Excelência operacional
  - Redefinir contas do Active Directory comprometidas
  - Substituir ponto de beacon obsoleto para StoreFront
  - Desabilitar URL de Serviços XenApp para lojas StoreFront
  - Descontinuar sites StoreFront não suportados
  - Desabilitar delegação Kerberos para lojas StoreFront

Esses aprimoramentos ajudam você a identificar proativamente problemas e tomar ações corretivas. Para mais informações, consulte Citrix Advisor.

Descarte granular para recomendações do Citrix Advisor. O Citrix Advisor agora oferece suporte ao descarte granular, permitindo que você descarte itens afetados específicos dentro de uma recomendação, em vez de ter que descartar a recomendação inteira. Esse aprimoramento é

útil para ambientes onde alguns recursos, como recursos de teste, validação ou temporários, devem se desviar das melhores práticas.

Ao descartar apenas itens intencionalmente não conformes, você pode reduzir o ruído enquanto mantém a visibilidade sobre problemas genuínos e continua a receber orientação de melhores práticas para seus recursos de produção.

Este recurso está disponível para os seguintes tipos de recursos:

- Catálogos de máquinas
- Grupos de entrega
- Grupos de aplicativos
- Zonas

Para mais informações, consulte Descartar itens afetados específicos em uma recomendação.

Personalizar regras de verificação do Advisor. Agora você pode personalizar as regras de verificação do Advisor para três recomendações principais:

- **Aprimorar o hardware do Cloud Connector:** Ajuste os limites para CPU, memória e uso de disco, e exclua discos específicos.
- **Liberar recursos não utilizados:** Defina limites de tempo de inatividade personalizados para máquinas e aplicativos.
- **Otimizar a configuração de GPO para VDAs:** Modifique a duração do tempo de processamento de GPO.

As recomendações personalizadas são rotuladas como **Personalizadas** para fácil identificação. Você pode reverter para as configurações padrão a qualquer momento. Para mais informações, consulte Personalizar regras de verificação do Advisor.

Controlar o comportamento de atualização de pacotes de aplicativos com Preferências. Agora você pode controlar como os pacotes de aplicativos são atualizados no fluxo de trabalho **Studio > Application Packages** usando as novas configurações de **Preferências**. Essas configurações permitem preservar os favoritos do usuário durante as atualizações, evitar downgrades não intencionais e remover automaticamente pacotes obsoletos durante as verificações de atualização. Isso ajuda você a manter um ambiente de aplicativo limpo e consistente com menos esforço manual.

Para obter mais informações, consulte Carregar pacotes de aplicativos em seu ambiente.

Visibilidade do Cloud Connector para VDAs. Agora você pode ver por quais Cloud Connectors seus VDAs são proxy em **Web Studio > Pesquisar**. Use a nova coluna e filtro **Cloud Connector** para visualizar e filtrar rapidamente os VDAs por Cloud Connector. Para exibir a coluna **Cloud Connector** na visualização principal de Pesquisa, selecione **Colunas a serem exibidas** no canto superior direito.

Adicionar notas para ações de energia. Agora você pode adicionar notas opcionais ao realizar ações de energia em máquinas e sessões. Essas notas ajudam você e outros administradores a entender o motivo da ação. Elas são registradas em logs para fins de auditoria. As notas são suportadas para as seguintes ações:

- **Ações da máquina**:
  - Iniciar
  - Desligar
  - Reiniciar
  - Forçar reinício
  - Forçar desligamento
- **Ações da sessão**:
  - Fazer logoff
  - Reiniciar (sessão única)
  - Desligar (sessão única)

Suporte para criação de catálogos Citrix Provisioning em ambientes de virtualização Red Hat OpenShift e Nutanix AHV Prism Central usando o Studio. Com o Studio, agora você pode criar catálogos Citrix Provisioning em ambientes de virtualização Red Hat OpenShift e Nutanix AHV Prism Central. Anteriormente, você tinha que alternar entre diferentes consoles para provisionar e gerenciar esses catálogos. Esse recurso simplifica o processo, permitindo que você execute tarefas de provisionamento e gerenciamento de energia inteiramente dentro do Studio. Para obter mais informações, consulte Criar catálogos Citrix Provisioning™ no Citrix Studio.

Tipos de disco Azure ZRS para imagens preparadas. O MCS no Azure agora permite que você selecione tipos de disco Zone Redundant Storage (`ZRS`) para imagens preparadas com gerenciamento de imagens MCS. Esse aprimoramento oferece maior flexibilidade na seleção do tipo de disco e melhora a resiliência de seus catálogos de máquinas MCS no Azure, garantindo maior disponibilidade para discos de imagem preparados.

Isso ajuda você a:

- Ter discos de imagem preparados com maior disponibilidade.
- Evitar o risco de perder imagens preparadas devido a interrupções de zona.
- Manter as operações em andamento sem impacto de falhas de disco do lado do armazenamento.

Para obter mais informações, consulte Criar uma imagem preparada.

Suporte para gerenciamento de imagens em ambientes Nutanix AHV Prism Central. A funcionalidade de gerenciamento de imagens agora está geralmente disponível para ambientes de virtualização OpenShift. Essa implementação reduz significativamente os custos de armazenamento e tempo, e simplifica o processo de implantação de VM e atualização de imagem. Atualmente, você também pode usar comandos PowerShell para atingir esse objetivo. Para obter informações, consulte Criar catálogos usando imagens preparadas no Nutanix AHV Prism Central.

Suporte para plug-in Amulet Hotkey CoreStation (Pré-visualização). Com este recurso, a Citrix gerencia suas cargas de trabalho Amulet Hotkey CoreStation por meio de um plug-in Amulet Hotkey CoreStation. Com este plug-in, você pode criar conexões de hospedagem para seu gabinete Amulet Hotkey CoreStation, criar catálogos e gerenciar o consumo de energia de máquinas no catálogo usando comandos PowerShell.

Para obter mais informações, consulte:

- Ambientes de virtualização Amulet Hotkey CoreStation
- Conexão com Amulet Hotkey CoreStation
- Criar um catálogo de máquinas Amulet Hotkey CoreStation
- Gerenciar o consumo de energia de VMs Amulet Hotkey CoreStation

Suporte para criação de catálogos de máquinas MCS habilitados para MCSIO de instâncias gerenciadas do Amazon WorkSpaces Core. Agora você pode criar catálogos MCS habilitados para MCSIO para criar catálogos de máquinas MCS habilitados para MCSIO de instâncias gerenciadas do Amazon WorkSpaces Core para melhorar o IOPS de gravação, direcionando as operações de gravação para o cache de write-back e para reduzir o tempo de inicialização quando o disco OS persistente está habilitado. Para obter mais informações, consulte Catálogo habilitado para MCSIO.

Gerenciar replicação de imagem local. Esta melhoria introduz um fluxo de trabalho explícito de replicação de imagem para hipervisores locais. Anteriormente, você não conseguia replicar instâncias de versão de imagem para locais de armazenamento recém-adicionados ou

substituídos, dificultando o gerenciamento da disponibilidade da imagem em todo o armazenamento necessário. Com esta melhoria, você pode executar comandos PowerShell e replicar a instância da versão da imagem para locais de armazenamento. Este recurso se aplica a hipervisores locais, incluindo ambientes VMware, XenServer e Nutanix AHV Prism Central.

Para obter mais informações, consulte Replicação de imagem de armazenamento adicional para hipervisores locais suportados.

Armazenamento SSD do Azure para discos de SO efêmeros. Este recurso aprimora o desempenho do disco de SO efêmero no Azure, permitindo que você selecione tipos de armazenamento SSD de nível superior. Anteriormente, apenas `Standard_LRS` era suportado. Agora, você pode usar `StandardSSD_LRS` ou `Premium_LRS` definindo a propriedade personalizada `StorageType` ao criar um catálogo MCS.

Isso ajuda você a:

- Alcançar um SLA mais alto com confiabilidade aprimorada.
- Experimentar IOPS significativamente mais altos em comparação com `Standard_LRS`.

Para obter mais informações, consulte Configurar o tipo de armazenamento usado por discos efêmeros.

Aprimorar a combinação de SKUs de backup do Azure. Este aprimoramento remove limitações anteriores no recurso `BackupVmConfiguration` do Azure. Anteriormente, não era possível misturar SKUs de VM que suportam hibernação com aqueles que não a suportam na mesma lista de backup. Esta atualização permite incluir SKUs capazes de hibernar e não capazes de hibernar em suas configurações de backup.

Isso ajuda você a:

- Usar uma gama mais ampla de SKUs de VM em suas configurações de backup.
- Melhorar as taxas de sucesso de provisionamento e inicialização de VMs no Azure.
- Aumentar a resiliência de suas implantações.

Para obter mais informações, consulte Configurar tamanhos de VM de backup.

Capacidade de ignorar os Cloud Connectors para solicitações de API do Amazon WorkSpaces Core. Ao usar instâncias gerenciadas do Amazon WorkSpaces Core, agora você pode configurar conexões de host para ignorar os Citrix Cloud Connectors para solicitações de API da AWS. Isso permite que o MCS se comunique diretamente do Delivery Controller para os

serviços da AWS para operações de provisionamento e gerenciamento de energia, em vez de rotear por meio de um proxy.

Este aprimoramento oferece maior flexibilidade operacional, reduz a carga de computação nas VMs do Cloud Connector e remove a dependência do MCS nos Cloud Connectors para solicitações de API da AWS. Para obter mais informações, consulte Ignorar Cloud Connectors para solicitações de API da AWS.

Alterar zonas de disponibilidade de VM do Azure. Este aprimoramento permite modificar a propriedade da zona de disponibilidade para VMs provisionadas pelo MCS existentes no Azure. Anteriormente, isso exigia a recriação da VM. Este recurso oferece maior flexibilidade, especialmente para máquinas virtuais persistentes.

Isso ajuda você a:

- Ajustar VMs do Azure existentes para não terem afinidade com zona de disponibilidade.
- Atribuir uma zona de disponibilidade específica a VMs do Azure que atualmente não possuem uma.
- Mover uma VM do Azure existente de uma zona de disponibilidade para outra.

Para obter mais informações, consulte Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento.

Suporte a GPU no OpenShift MCS. O OpenShift MCS atualmente oferece suporte à configuração de GPU por meio do comportamento de passthrough. As configurações de GPU definidas na VM mestre ou no Perfil da Máquina são lidas e aplicadas às VMs provisionadas por meio do catálogo MCS. Atualmente, você não pode modificar os parâmetros de GPU durante a criação do catálogo. A configuração de GPU é herdada diretamente da configuração de origem e aplicada às VMs provisionadas conforme configurado.

Faturamento flexível para instâncias gerenciadas do Amazon WorkSpaces Core. Agora você pode escolher entre os modelos de faturamento Mensal (taxa fixa) e Horário (pague conforme o uso) ao provisionar instâncias gerenciadas do Amazon WorkSpaces Core usando o Citrix MCS.

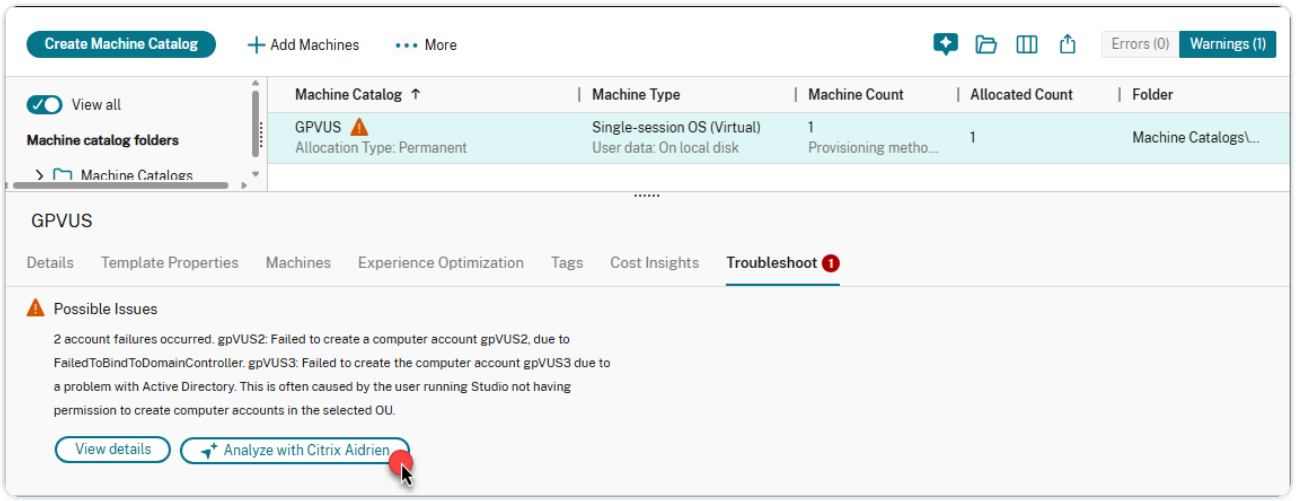
Essa flexibilidade permite otimizar os custos de computação com base nos requisitos específicos da sua carga de trabalho e nos padrões de uso.

Use o modo de faturamento Mensal para desktops persistentes para se beneficiar de preços previsíveis e de taxa fixa, ou use o faturamento Horário para cargas de trabalho sob demanda ou intermitentes.

Este recurso exige que sua conta AWS esteja configurada para o serviço de faturamento do Amazon WorkSpaces.

Para obter mais informações, consulte Faturamento flexível.

Solução de problemas com o Citrix Aidrien. Agora você pode solucionar avisos e erros no Citrix DaaS usando o Citrix Aidrien. Quando avisos ou erros ocorrem, o Aidrien está disponível diretamente na guia **Solução de problemas**, em pop-ups de aviso e erro, e no centro de Notificações. O Aidrien analisa os problemas no contexto e fornece insights guiados para ajudar você a diagnosticar e resolver problemas mais rapidamente. Para obter mais informações, consulte Casos de uso do Citrix DaaS.



AWS EC2: Compartilhe imagens AWS preparadas entre regiões. Agora você pode compartilhar uma imagem preparada de uma região para uma ou mais regiões diferentes dentro da mesma conta AWS. Este recurso está disponível para ambientes AWS EC2. Ao compartilhar uma imagem, a AMI subjacente é copiada junto com suas propriedades, como criptografia, hibernação, tags e inicialização confiável. Isso ajuda você a:

- Implantar e gerenciar imagens preparadas em diferentes regiões de forma eficiente.
- Criar ou atualizar catálogos de máquinas em várias regiões usando as imagens preparadas compartilhadas.
- Manter configurações de imagem consistentes em sua implantação AWS.

Para obter mais informações, consulte Compartilhar imagens preparadas entre zonas de disponibilidade e regiões.

AWS EC2: Provisionar cargas de trabalho em zonas locais da AWS. Agora você pode provisionar cargas de trabalho do AWS EC2 diretamente em zonas locais da AWS. Este novo recurso ajuda você a:

- Fornecer acesso de baixa latência para usuários finais implantando cargas de trabalho Citrix mais próximas a eles.
- Melhorar a cobertura regional para sua infraestrutura Citrix em áreas não atendidas por Regiões AWS completas.

Você pode criar uma conexão de host com uma unidade de hospedagem em uma zona local desejada e, em seguida, provisionar VMs nessa zona local.

Para obter mais informações, consulte:

- Criar uma conexão usando o Studio
- Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Suporte para criação de catálogos do Citrix Provisioning (PVS) usando comandos do PowerShell do MCS com conexão Nutanix AHV Prism Central. Agora você pode criar catálogos do Citrix Provisioning usando comandos do PowerShell do MCS na conexão de host Nutanix AHV Prism Central. Esta implementação oferece as seguintes vantagens:

- Uma única API unificada para gerenciar catálogos MCS e Citrix Provisioning.
- Ter novos recursos para catálogos do Citrix Provisioning, como solução de gerenciamento de identidade, provisionamento sob demanda e outros.

Para obter mais informações, consulte documentação do PVS.

Março de 2026

Recursos novos e aprimorados

Logon único do Microsoft Entra para DaaS. As seguintes melhorias estão disponíveis:

- O suporte para acesso híbrido no Linux agora está disponível com o aplicativo Citrix Workspace para Linux 2601.
- Agora você pode registrar os aplicativos Citrix Resource e Client através do portal Citrix Cloud.
- Agora você pode realizar a configuração do Azure através do portal do Azure.

Para obter mais informações, consulte Logon único do Microsoft Entra.

Suporte para atributos de extensão do Entra ID no MCS. Agora você pode integrar atributos de extensão do Entra ID ao seu ambiente MCS. Esses atributos permitem que você armazene dados exclusivos e personalizados diretamente nos objetos de dispositivo do Entra ID. Assim, você pode aplicar políticas de acesso condicional precisas filtrando dispositivos com atributos de extensão.

Consulte Operadores suportados e propriedades de dispositivo para filtros para criar mais filtros com base nos atributos do dispositivo. O recurso é suportado para tipos de identidade unidos ao Microsoft Entra e unidos ao Microsoft Entra híbrido.

Você pode gerenciar seus catálogos de máquinas MCS usando atributos de extensão do Entra ID (ExtensionAttribute1-15). Para isso, prepare um Service Principal com permissão `Device.ReadWrite.All`. Você pode criar e atualizar um catálogo de máquinas MCS com atributos de extensão do Entra ID usando comandos do Studio e do PowerShell.

Os atributos de extensão são atribuídos aos dispositivos (VMs persistentes e não persistentes) quando são registrados.

Para obter mais informações, consulte:

- Pool de identidade de máquina unida ao Microsoft Entra
- Pool de identidade de máquina unida ao Microsoft Entra híbrido
- Criar catálogos do Microsoft Entra registrados no Microsoft Intune
- Criar catálogos unidos ao Microsoft Entra híbrido registrados no Microsoft Intune

Nutanix AHV Prism Central: Melhorar a configuração de rede. Esta melhoria aprimora a configuração de rede para catálogos MCS em conexões de host do Nutanix AHV Prism Central. Agora você pode configurar as configurações de rede distinguindo claramente entre VLANs Básicas, VLANs Avançadas e redes de Sobreposição, evitando erros que ocorriam quando tipos mistos eram listados juntos anteriormente.

Isso ajuda você a:

- Reduza erros durante os processos de criação e edição de catálogos de máquinas.
- Garanta configurações de rede consistentes e válidas por meio de novas verificações pré-voo.

Para obter mais informações, consulte Criar um catálogo de máquinas usando o Studio.

Compartilhe versões de imagens preparadas entre hosts no mesmo pool de recursos no XenServer. Agora você pode usar o nó **Imagens** para compartilhar versões de imagens entre hosts no mesmo pool de recursos no XenServer. Essa implementação garante a consistência e a uniformidade das imagens em diferentes hosts, aprimorando a flexibilidade de implantação e a eficiência operacional. Você também pode usar comandos PowerShell para atingir esse objetivo. Para obter mais informações, consulte Criar um catálogo de máquinas de imagem preparada no XenServer.

Citrix Advisor: Nova verificação de confiabilidade. O Citrix Advisor agora inclui uma nova verificação de ambiente com a recomendação **Habilitar continuidade do serviço para Citrix Workspace**. Essa verificação identifica quando a continuidade do serviço não está habilitada e fornece orientação para ajudá-lo a habilitá-la. Para obter mais informações, consulte Recomendações de confiabilidade.

Personalizar layout de coluna nas visualizações principais da Pesquisa. Agora você pode reordenar colunas no Web Studio para organizar e agrupar melhor as informações relacionadas. O Web Studio retém suas preferências de ordem e largura de coluna, para que seu layout personalizado persista entre as sessões. Atualmente, essa capacidade é suportada nas visualizações principais em **Pesquisa**.

Janela de Serviço. O recurso Janela de Serviço oferece a capacidade de agendar e automatizar operações em VMs provisionadas por MCS. Atualmente, esse recurso suporta várias operações, como redefinição de disco do sistema operacional e alterações de configuração de hardware usando PowerShell. Para obter informações, consulte Janela de Serviço.

Fevereiro de 2026

Recursos novos e aprimorados

O Monitor agora suporta a execução de Tarefas Scripted. Isso inclui a capacidade de executar scripts integrados do Citrix e scripts personalizados, bem como fazer upload de scripts personalizados para execução. Esse aprimoramento permite que os administradores realizem a solução de problemas e automatizem tarefas operacionais diretamente do Monitor.

Rastreamento Sempre Ativo do Citrix. O Citrix Cloud expande o Rastreamento Sempre Ativo (AOT) para simplificar a coleta centralizada de logs para Citrix Virtual Apps and Desktops. A configuração é gerenciada por meio das Configurações do DaaS, onde os administradores definem os detalhes do Servidor de Log, o escopo de log e os controles de acesso, com as configurações aplicadas em todo o ambiente.

O Citrix Monitor adiciona uma visualização dedicada de Logs AOT com visibilidade quase em tempo real, pesquisa e filtragem por intervalo de tempo, tipo de log e máquina para acelerar a solução de problemas.

Os logs AOT são enviados para o Servidor de Log AOT a partir de componentes suportados implantados em locais de recursos do cliente, incluindo VDAs Windows, Linux e Mac, StoreFront, Federated Authentication Service (FAS) e Session Recording Server.

Para obter mais informações, consulte Rastreamento Sempre Ativo.

Nota:

Os logs AOT dos componentes do plano de controle do Citrix Cloud continuam sendo enviados para sistemas de monitoramento gerenciados pela Citrix, como o Splunk. Somente os componentes implantados em locais de recursos do cliente enviam logs para o Servidor de Logs AOT.

Logon único do Microsoft Entra para DaaS. O suporte para acesso híbrido no Windows e Mac agora está disponível. Consulte Logon único do Microsoft Entra para obter detalhes.

Configuração de VM de backup no AWS EC2. O Studio agora permite que você defina uma lista de tipos de instância EC2 de backup (“SKUs de Backup” que podem ser instâncias sob demanda ou spot) em ambientes AWS para os quais o Machine Creation Services (MCS) pode recorrer em caso de problemas relacionados à capacidade. O MCS tenta recorrer aos tipos de instância EC2 de backup na ordem fornecida por você na lista. Para obter mais informações, consulte Criar um catálogo usando o Studio.

Suporte para Zonas Estendidas do Azure. Agora você pode provisionar cargas de trabalho em Zonas Estendidas do Azure usando o provisionamento MCS. As Zonas Estendidas do Azure são extensões de pequena pegada das principais regiões do Azure. Elas fornecem menor latência e residência de dados para clientes que estão mais distantes do local da região principal. Para obter mais informações, consulte Zonas Estendidas do Azure.

Red Hat OpenShift: Catálogo de Provisionamento Citrix usando MCS. Este aprimoramento adiciona suporte ao Plug-in do OpenShift para provisionar catálogos do Citrix Provisioning (PVS) usando MCS.

Com essa capacidade:

- O Plug-in do OpenShift pode ser usado como uma conexão de hospedagem para catálogos de máquinas do Citrix Provisioning provisionados pelo MCS.
- Os dispositivos de destino do Citrix Provisioning podem inicializar usando a inicialização BDM do Citrix Provisioning, com o disco BDM armazenado no OpenShift.

Para obter mais informações, consulte o documento do Citrix Provisioning Criar catálogos do Citrix Provisioning™ no Citrix Studio.

Registrar máquinas HPE Moonshot em catálogos de máquinas usando WebSocket. Agora você pode registrar seus VDAs não associados a domínio ou associados ao Microsoft Entra no HPE Moonshot em catálogos de máquinas usando WebSocket. Para obter mais informações, consulte Registrar máquinas em catálogos usando a ferramenta de registro de VDA WebSocket.

Suporte para VMware vVols no MCS. Agora você pode usar VMware vVols com MCS em ambientes vSphere. Anteriormente, a criação de catálogos MCS em vVols resultava em erros de PBM. Esta atualização resolve esse problema. Esta integração fornece controle granular sobre o armazenamento de sua máquina virtual MCS. Para obter informações, consulte Perfil de Armazenamento.

Usar configurações de servidor proxy WinHttp (netsh) para conexão de hospedagem. Este recurso permite que as conexões de hospedagem usem as configurações de servidor proxy WinHttp (netsh) configuradas nos Citrix Cloud Connectors para serem usadas com a conexão de hospedagem. Para obter mais informações, consulte Usar configurações de servidor proxy WinHttp (netsh) para conexão de hospedagem.

Instâncias Gerenciadas do Amazon Workspaces Core: Provisionamento entre contas usando PowerShell. Existem casos de uso em que os Cloud Connectors gostariam de ser colocados em uma conta AWS separada (conta de serviços compartilhados ou conta de componentes de site) com funções IAM que têm acesso entre contas (função IAM entre contas) e catálogos de máquinas provisionados por MCS em uma conta AWS secundária separada (contas de cargas de trabalho), sem a necessidade de Cloud Connectors adicionais nas contas separadas. Para suportar tais cenários, este recurso usa o emparelhamento de VPC e o acesso entre contas usando funções IAM para tornar o provisionamento entre diferentes contas AWS possível para empresas que gerenciam várias contas AWS.

Com emparelhamento de VPC, você pode fazer com que seu Cloud Connector e VMs provisionadas em diferentes regiões ou contas possam se comunicar entre si.

Com acesso entre contas usando funções IAM, você permite que a conta primária (conta do Cloud Connector) assuma uma função IAM para acessar recursos AWS na conta secundária (VMs do catálogo de máquinas).

Para informações detalhadas, consulte Provisionamento entre contas.

Amazon Workspaces Core Managed Instances: Provisione cargas de trabalho em zonas locais da AWS. Agora você pode provisionar cargas de trabalho do Amazon Workspaces Core Managed Instances diretamente em zonas locais da AWS. Este novo recurso ajuda você a:

- Fornecer acesso de baixa latência para usuários finais implantando cargas de trabalho Citrix mais perto deles.
- Melhorar a cobertura regional para sua infraestrutura Citrix em áreas não atendidas por regiões AWS completas.
- Você pode criar uma conexão de host com uma unidade de hospedagem em uma zona local desejada e, em seguida, provisionar VMs nessa zona local.

Para obter mais informações, consulte:

- Criar uma conexão usando o Studio
- Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Amazon WorkSpaces Core Managed Instances: Compartilhe imagens AWS preparadas entre regiões. Agora você pode compartilhar uma imagem preparada de uma região para uma ou mais regiões diferentes dentro da mesma conta AWS. Este recurso está disponível para ambientes Amazon Workspaces Core Managed Instances. Ao compartilhar uma imagem, a AMI subjacente é copiada junto com suas propriedades, como criptografia, tags e inicialização confiável. Isso ajuda você a:

- Implantar e gerenciar imagens preparadas em diferentes regiões de forma eficiente.
- Criar ou atualizar catálogos de máquinas em várias regiões usando as imagens preparadas compartilhadas localmente.
- Manter configurações de imagem consistentes em sua implantação AWS.

Para obter mais informações, consulte Compartilhar imagens preparadas entre zonas de disponibilidade e regiões.

Suporte expandido a ícones. Ao personalizar ícones para desktops e aplicativos no Studio, agora você pode extrair e usar ícones de arquivos `.exe`, além do formato `.ico` suportado anteriormente.

Você pode navegar e selecionar esses ícones de sua máquina local ou de uma máquina VDA. O tamanho máximo de arquivo de ícone suportado é de 500 KB. Para obter mais informações, consulte Criar grupos de entrega e Gerenciar grupos de entrega.

Citrix Advisor: Novas verificações para confiabilidade, desempenho, segurança e eficiência de custos. O Citrix Advisor agora inclui as seguintes novas verificações de ambiente que fornecem recomendações acionáveis para ajudar a melhorar a segurança, confiabilidade, desempenho e excelência operacional:

- Segurança
  - Usar HTTPS para conexões de host
  - Atualizar sistemas operacionais que atingiram o Fim da Vida Útil
  - Atualizar versões de hipervisor que atingiram o Fim da Vida Útil
- Confiabilidade
  - Habilitar verificação de integridade avançada para lojas StoreFront
  - Adicionar todos os Cloud Connectors como servidores STA no StoreFront e NetScaler Gateway
- Desempenho
  - Otimizar a configuração de GPO para VDAs
  - Avaliar o tamanho do disco de cache de gravação para dispositivos de destino PVS
- Excelência operacional
  - Simplificar a configuração do catálogo com um perfil de máquina

Esses aprimoramentos permitem que você identifique proativamente problemas e tome ações corretivas para manter uma implantação segura, confiável, de alto desempenho e operacionalmente eficiente. Para obter mais informações, consulte Citrix Advisor.

Encaminhar logs de Rastreamento Sempre Ativo (AOT) para o seu servidor de log. No Web Studio, agora você pode encaminhar logs de Rastreamento Sempre Ativo (AOT) de componentes Citrix para um servidor de log designado. Este recurso permite a solução de problemas centralizada e um monitoramento mais eficaz do seu ambiente Citrix. Para obter mais informações, consulte Configurar as configurações do servidor de log.

Migrar catálogos de máquinas para a conexão de host do Nutanix AHV Prism Central gerenciada pela Citrix. Com esse recurso, você pode migrar seus catálogos de máquinas Citrix e suas VMs associadas das conexões de host existentes do Nutanix AHV (para Prism Element) e Nutanix AHV PC (para NC2 no Azure) para a conexão de host do Nutanix AHV Prism Central gerenciada pela Citrix. Para a migração, use comandos do PowerShell, que também incluem opções de reversão rápida em caso de problemas e comandos para limpar os recursos de origem após a migração. Para obter informações, consulte Migrar catálogos de máquinas para a conexão de host do Nutanix AHV Prism Central gerenciada pela Citrix.

Usar perfis de máquina para conexões de host do Nutanix AHV Prism Central. Agora você pode usar perfis de máquina para definir configurações de hardware para VMs provisionadas por meio de sua conexão de host do Nutanix AHV Prism Central. Este novo fluxo de trabalho captura propriedades como CPU, memória, núcleos por soquete, GPU e categorias do perfil da máquina. Você pode substituir as configurações de CPU, memória e núcleos por soquete durante a criação ou edição do catálogo. A versão do modelo da imagem mestre é definida como o perfil da máquina para novos catálogos. Você pode criar um novo catálogo com um perfil de máquina, atualizar um catálogo existente e converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina usando o Studio e o PowerShell. Para obter mais informações, consulte:

- Studio
  - Criar um catálogo de máquinas usando o Studio
  - Adicionar ou alterar o perfil da máquina.
- PowerShell
  - Criar um catálogo de máquinas usando comandos do PowerShell
  - Adicionar ou alterar perfil da máquina

Desktops agrupados de uso único durante eventos LHC. Desktops agrupados, de sessão única e gerenciados por energia agora estão disponíveis para uso único por padrão durante um evento de Cache de Host Local (LHC). Essa alteração garante que os usuários possam acessar essas máquinas sem preocupações com a reutilização do desktop. A funcionalidade existente para configurar esses desktops para reutilização permanece inalterada. Para obter mais informações, consulte Habilitar usando o Studio.

Janeiro de 2026

Recursos novos e aprimorados

Descobrir e entregar camadas de aplicativos elásticas Citrix no Studio. Agora você pode descobrir e publicar camadas de aplicativos elásticas usando o nó **Pacotes de aplicativos** no Studio, incluindo:

- Descobrir e enumerar uma biblioteca de camadas de aplicativos elásticas criadas usando o Citrix App Layering.
- Criar políticas de atribuição para entregar aplicativos elasticamente aos usuários em catálogos de máquinas não persistentes.

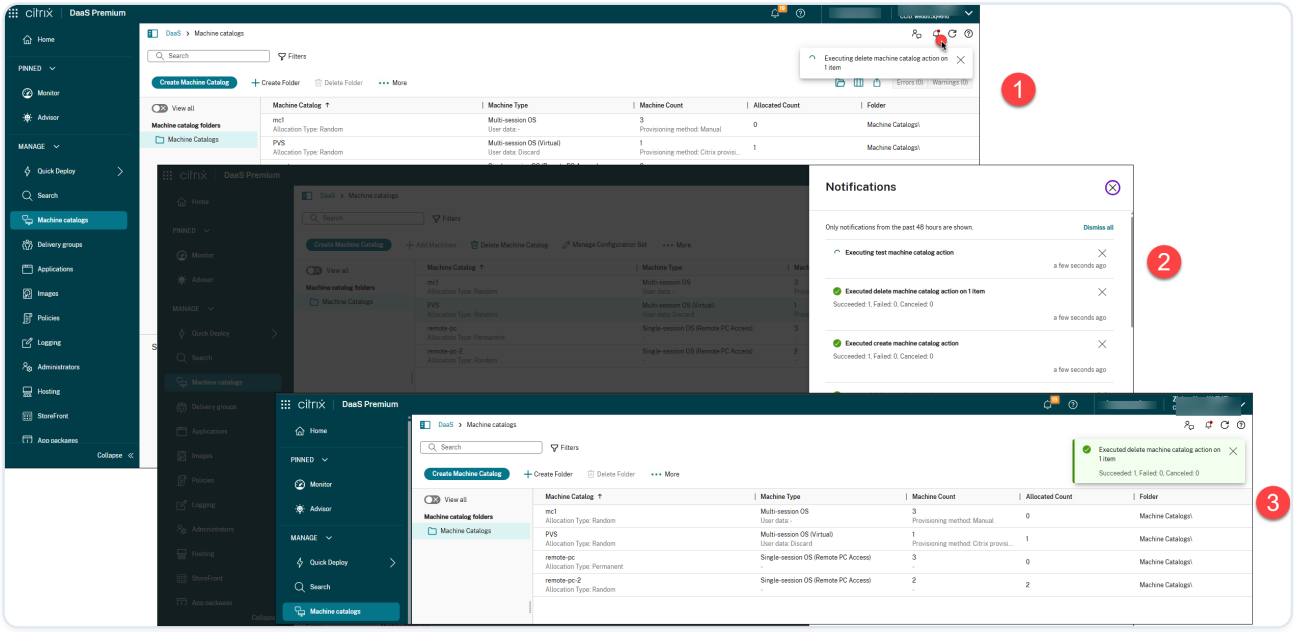
- Entregar camadas de aplicativos elásticas portáteis para qualquer máquina Windows não persistente, independentemente de a imagem ter sido publicada a partir de um dispositivo App Layering.

Para mais informações, consulte Gerenciar pacotes de aplicativos.

Notificações em sessão para operações em segundo plano. O Web Studio agora inclui um centro de notificações que oferece visibilidade em tempo real das operações em segundo plano e relatórios sobre os resultados das operações.

Quando você inicia uma operação demorada, uma notificação aparece no canto superior direito para informar que ela está em andamento. As operações que antes bloqueavam a interface do usuário agora são executadas em segundo plano, para que você possa continuar trabalhando sem interrupção. Assim que a operação é concluída, uma notificação de status em tempo real aparece, e o resultado também é salvo no centro de notificações. O centro de notificações mantém um histórico de 48 horas, facilitando o rastreamento de atividades recentes.

Para mais informações, consulte Visão geral do Studio.



Logon único do Microsoft Entra para DaaS. O suporte com as novas plataformas do aplicativo Workspace e o Windows Server 2025 já está disponível. Consulte Logon único do Microsoft Entra para obter detalhes.

Marcação follow-me. A marcação follow-me permite o rastreamento do uso individual de VMs por usuários finais, aplicando tags no nível do hipervisor. Essas tags, rotuladas com o usuário e/ou organização específicos (usando `citrix-user-upn` como chave e o Nome Principal do Usuário

(UPN) como valor), são adicionadas quando um usuário é atribuído a uma VM e removidas quando o usuário é desatribuído.

Este recurso oferece várias vantagens:

- **Rateio de TI**: Facilita a filtragem do uso de recursos (Azure: NICs, OS, ID, WBC, discos de dados e VMs) (AWS EC2: instância EC2, volumes EBS (OS, ID, WBC e discos de dados), interfaces de rede) por tags, permitindo um rateio preciso para usuários individuais ou unidades de negócios.
- **Gerenciamento eficiente de usuários**: Automatiza a remoção de tags de recursos quando os usuários finais são desatribuídos devido a mudanças de emprego, como rescisão ou reorganização.
- **Monitoramento de segurança aprimorado**: Ajuda a identificar VMs atribuídas a usuários finais específicos para verificações de segurança direcionadas.

Atualmente, a marcação follow-me é aplicável a:

- Ambientes AWS EC2 e Azure
- Máquinas atribuídas estaticamente executando SO de sessão única
- Catálogos persistentes e não persistentes
- Todos os catálogos com identidade de máquina associada suportados
- Apenas VMs provisionadas por MCS
- Apenas discos gerenciados

Para obter mais informações, consulte Marcação Follow-Me.

Suporte para provisionamento de disco de dados na AWS. Um disco de dados permite o armazenamento de dados persistentes, como logs de eventos, rastreamentos de segurança e dados de aplicativos.

Com este recurso, agora você pode criar e atribuir um disco de dados persistente a uma VM persistente ou não persistente criada por MCS de um catálogo de máquinas MCS na AWS. A origem do disco de dados deve ser a imagem mestre (volume secundário da AMI). Você pode provisionar o disco de dados usando comandos do Studio e do PowerShell. No entanto, você pode provisionar discos de dados usando a interface do usuário do Studio apenas quando a imagem mestre (AMI) tiver dois volumes, disco do SO (volume raiz) e disco de dados (volume secundário).

Para obter informações sobre como criar um catálogo de máquinas MCS com um disco de dados, consulte Provisionar um disco de dados em uma VM criada por MCS.

Dezembro de 2025

Recursos novos e aprimorados

Azure: Clonar catálogos MCS. Agora você pode usar o comando PowerShell `Copy-ProvScheme` para clonar um catálogo de máquinas MCS persistente e não persistente existente no ambiente de virtualização do Azure. Este recurso cria um novo esquema de provisionamento copiando os detalhes de um esquema existente, incluindo configurações associadas, mapeamentos de rede e grupos de segurança. Isso ajuda você a:

- Dividir um catálogo único existente em vários catálogos para aplicar diferentes políticas e configurações em nível de catálogo.
- Isolar máquinas virtuais específicas dentro de um catálogo grande para testes rápidos ou para tratá-las separadamente com base em funções funcionais.

Para obter mais informações, consulte Clonar um catálogo MCS.

Configurações aprimoradas de otimização de experiência para Citrix DaaS. Aprimoramos as configurações de **Otimização de Experiência** para ajudar você a ajustar facilmente a alocação de recursos e aumentar o desempenho em catálogos de máquinas. Agora você pode criar ou selecionar conjuntos de configuração para otimização personalizada, ou aplicar rapidamente configurações padrão como proteção automática contra picos de CPU e otimização inteligente de CPU.

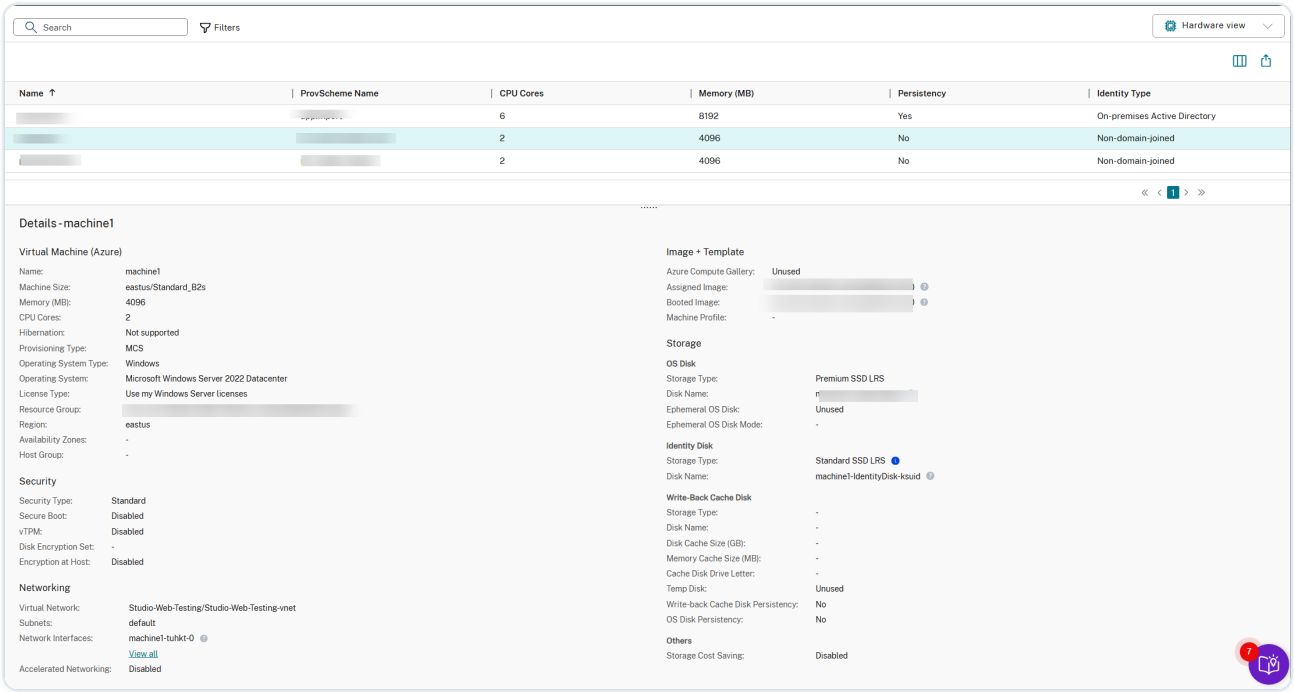
Para obter mais informações, consulte Selecionar um conjunto de configuração para otimização de experiência.

Visualização de hardware da máquina no nó de Pesquisa. Agora você pode acessar uma visualização de hardware dedicada no nó de Pesquisa para máquinas provisionadas usando o Machine Creation Services (MCS). Essa visualização oferece melhor visibilidade dos detalhes de hardware da máquina e facilita o gerenciamento de máquinas provisionadas por MCS.

Os principais benefícios incluem:

- Visualize configurações detalhadas de hardware, incluindo tamanho da máquina, sistema operacional, tipo de licença, configurações de segurança, rede, imagem, modelo e configurações de disco.
- Localize facilmente máquinas usando filtros de hardware e opções de pesquisa.

Atualmente, a visualização de Hardware está disponível para máquinas provisionadas por MCS em VMware, XenServer, SCVMM/Hyper-V, Nutanix PC, Azure, Azure Arc, Azure Local, AWS EC2 e GCP. OpenShift e Amazon WorkSpaces Core atualmente mostram informações básicas de hardware apenas como colunas. Para obter mais informações, consulte Monitorar máquinas provisionadas por MCS em Pesquisa > Visualização de hardware.



Controle de escopo aprimorado para o Conjunto de Políticas Padrão. O controle de escopo está disponível para conjuntos de políticas. Para manter a compatibilidade, o **Conjunto de Políticas Padrão** agora é atribuído a *qualquer* escopo, com o **Controle de escopo de bypass** habilitado por padrão. Revise suas atribuições do **Conjunto de Políticas Padrão** e ajuste-as se quiser limitar o acesso com base no escopo.

Você pode atualizar as atribuições de escopo de duas maneiras:

- Nas políticas: Edite o **Conjunto de Políticas Padrão** e altere seus escopos associados.
- No escopo: Vá para o escopo em **Administradores > Escopos** e atribua ou remova o **Conjunto de Políticas Padrão** dele.

Para obter mais informações, consulte Criar e gerenciar escopos e Criar e gerenciar conjuntos de políticas.

Relocação do nó StoreFront. O nó **StoreFront** foi removido do Web Studio. Todas as configurações e opções de configuração anteriormente disponíveis no nó **StoreFront** agora estão disponíveis na guia **Configurações** do nó **Grupos de entrega**. Essa consolidação simplifica a navegação e mantém as opções de configuração relacionadas em um só lugar.

AWS EC2: Compartilhar imagens preparadas entre zonas de disponibilidade. Anteriormente, para criar catálogos de máquinas MCS em várias zonas de disponibilidade, você precisava de uma imagem preparada separada para cada zona de disponibilidade. Isso aumentava sua complexidade operacional, pois você precisava gerenciar várias imagens preparadas e poderia levar a inconsistências potenciais no gerenciamento de imagens.

Com esse recurso, você pode compartilhar uma única imagem preparada entre diferentes zonas de disponibilidade na mesma região da AWS para o AWS EC2. Isso simplifica a criação de catálogos e as atualizações de imagens, reduzindo significativamente a sobrecarga de gerenciamento. Atualmente, use comandos PowerShell para gerenciar o compartilhamento de imagens. Para obter mais informações, consulte Compartilhar imagens preparadas entre zonas de disponibilidade.

Criar VMs provisionadas por MCS com vTPM habilitado no XenServer 8. Com esse recurso no XenServer 8, você pode criar um catálogo de máquinas MCS com vTPM. Se a configuração baseada em perfil de máquina for usada e o vTPM estiver habilitado, as VMs no catálogo herdarão o mesmo conteúdo vTPM do modelo de VM. Se o perfil da máquina não for usado e a imagem mestre tiver o vTPM habilitado, as VMs no catálogo herdarão o mesmo conteúdo vTPM da imagem mestre. Para obter informações, consulte Criar um catálogo de máquinas baseado em perfil de máquina usando PowerShell.

Novembro de 2025

Recursos novos e aprimorados

Logon único do Microsoft Entra para DaaS. Agora você pode aproveitar o logon único (SSO) ao usar credenciais do Microsoft Entra ID para acessar aplicativos e desktops virtuais em hosts de sessão ingressados no Microsoft Entra ou híbridos ingressados no Microsoft Entra. Para obter mais informações, consulte Logon único do Microsoft Entra.

Instâncias gerenciadas do Amazon WorkSpaces Core: Compartilhe imagens preparadas entre zonas de disponibilidade usando a interface do usuário do Studio. Com este recurso, você pode compartilhar uma única imagem preparada entre diferentes zonas de disponibilidade na mesma região da AWS para instâncias gerenciadas do Amazon WorkSpaces Core usando a interface do usuário do Studio. Alternativamente, você também pode usar comandos do PowerShell para gerenciar o compartilhamento de imagens. Para obter mais informações, consulte Compartilhar imagens preparadas entre zonas de disponibilidade.

Desktops agrupados de uso único no Cache do Host Local. Agora você pode configurar o uso único de desktops agrupados durante o modo de interrupção do Cache do Host Local (LHC). Ele

aproveita um blob de higiene distribuído apenas para VDAs versão 2407 e posteriores. Máquinas capazes são automaticamente agendadas para reinicialização após uma única sessão de interrupção para garantir um estado limpo. Este recurso melhora o sentimento do cliente durante interrupções, tornando a disponibilidade mais contínua. Para obter mais informações, consulte Desktops agrupados de uso único no Cache do Host Local.

Gerenciando versões de imagens preparadas no AWS EC2. A funcionalidade de gerenciamento de imagens agora está geralmente disponível para ambientes de virtualização AWS EC2. Você pode usar o nó **Imagens** para criar várias versões de imagem e aplicar ou atualizar vários catálogos de máquinas. Esta implementação reduz significativamente os custos de armazenamento e tempo e simplifica o processo de implantação de VM e atualização de imagem. Você também pode usar comandos do PowerShell para atingir este objetivo. Para obter mais informações, consulte Criar um catálogo de máquinas de imagem preparada no AWS EC2.

Instâncias gerenciadas do Amazon WorkSpaces Core: suporte para não-ingresso no domínio na interface do usuário do Studio. Anteriormente, a interface do usuário do Studio suportava Active Directory local e Microsoft Entra híbrido ingressado para instâncias gerenciadas do Amazon WorkSpaces Core, mas não suportava o provisionamento de configurações não ingressadas no domínio.

Com este aprimoramento, você pode provisionar instâncias gerenciadas do Amazon WorkSpaces Core que não estão ingressadas no domínio diretamente na interface do usuário do Studio usando MCS. Esta funcionalidade é suportada durante as fases de criação e edição de catálogos de máquinas MCS na interface do usuário do Studio. Para obter informações, consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas.

Azure: Suporte a tamanhos de VM de backup entre famílias para VMs Hibernadas. O MCS no Azure agora suporta o uso de tamanhos de VM entre famílias para configurações de backup em catálogos de máquinas habilitados para hibernação, melhorando a resiliência. Este recurso remove a restrição anterior que bloqueava o fallback entre famílias para evitar erros de tela azul ao retomar. Quando ocorre uma falha de alocação ao retomar uma VM hibernada, o MCS lida automaticamente com a mudança de tamanho, garantindo que você ainda obtenha uma VM funcional. Observe que a mudança do tamanho da VM requer a limpeza do estado hibernado, resultando na perda do estado de memória da VM (dados da RAM). Esta funcionalidade está disponível para catálogos MCS persistentes e não persistentes. Para obter mais informações, consulte Configurar tamanhos de VM de backup.

Dimensionamento de carga de trabalho aprimorado. A página de dimensionamento de carga de trabalho aprimorado ajuda você a analisar os aspectos de uso e dimensionamento dos seus

grupos de entrega. Assim, os grupos de entrega podem ser analisados com base na atividade da máquina ou do usuário.

A análise baseada em máquina permite que você:

- Categorizar desktops virtuais com base no uso para identificar máquinas com nenhuma ou baixa atividade e reduzir gastos com recursos não utilizados. Para obter mais informações, consulte Análise de Uso
- Analisar a utilização de recursos em desktops virtuais para identificar máquinas que precisam ser dimensionadas corretamente para reduzir custos ou melhorar a experiência do usuário. Para obter mais informações, consulte Análise de Dimensionamento

A análise baseada no usuário permite que você:

- Categorizar os usuários com base em sua atividade. Considere remover o direito de acesso de usuários sem atividade por razões de higiene de TI. Usuários com baixo uso poderiam ser movidos para recursos compartilhados para um uso mais eficiente dos recursos.
- Analise o consumo de recursos dos usuários para identificar grupos com consumo de recursos acima ou abaixo da média e para distribuir os usuários de forma mais eficaz.

A análise de máquinas é ideal para cenários com desktops virtuais atribuídos estaticamente aos usuários, como Windows 365 Enterprise ou Frontline dedicado. A análise de usuários é útil para a análise de grupos de entrega com desktops virtuais atribuídos aleatoriamente. Ambas as análises estão atualmente limitadas a máquinas de sessão única.

> **Nota:**
>
> A análise clássica de dimensionamento correto (rightsizing), acessível através do botão “Todas as cargas de trabalho” na parte superior da página, será descontinuada em uma próxima versão.

> **Visualize usuários bloqueados por falhas no lançamento de sessão**. Os administradores agora têm **visibilidade dos usuários bloqueados por falhas no lançamento de sessão**. Este novo resumo está disponível em **Filtros** na visualização **Conexões**, permitindo melhor priorização e análise de falhas.

As tendências de desempenho da sessão agora estão disponíveis com personalização. As tendências de desempenho da sessão no Citrix Director suportam dados históricos. Os

administradores agora podem personalizar as métricas para correlacionar a partir de uma lista enriquecida de métricas de desempenho.

Insights de diagnóstico em máquinas e sessões para monitoramento proativo. O Citrix Director agora apresenta um painel de Insights para ajudar os administradores a identificar e resolver proativamente falhas de sessão e problemas de desempenho. Esta poderosa ferramenta fornece insights de diagnóstico, atualizados a cada 15 minutos, para destacar máquinas e sessões problemáticas que afetam seu site.

Os principais insights incluem:

- Máquinas Black Hole: Detecta máquinas que falham ao atender solicitações de sessão consecutivas
- Sessões zumbis: Identifica máquinas de SO de sessão única com sessões abandonadas que bloqueiam novos lançamentos de sessão.
- Máquinas sobrecarregadas: Sinaliza máquinas com picos sustentados de CPU ou memória que estão degradando a experiência do usuário.
- Falhas de conexão: Destaca falhas de cliente e servidor, fornecendo detalhes sobre padrões de falha e impacto no usuário.

Os insights são personalizáveis, com políticas de alerta que podem ser configuradas para notificação. Os insights capacitam os administradores a serem proativos, agirem em tempo hábil e melhorarem a disponibilidade e o desempenho da sessão em seu ambiente. Para obter mais informações, consulte Insights

Outubro de 2025

Recursos novos e aprimorados

Citrix Advisor: Novas verificações para confiabilidade, desempenho, segurança e eficiência de custos. O Citrix Advisor agora inclui as seguintes novas verificações de ambiente que fornecem recomendações acionáveis para ajudar a melhorar a confiabilidade, o desempenho, a segurança e a eficiência de custos:

- **Confiabilidade**
  - Habilitar a comunicação entre os Cloud Connectors para um desempenho LHC confiável
  - Colocar os Cloud Connectors no mesmo domínio
  - Verificar as configurações de resiliência

- **Desempenho**
  - Dimensionar corretamente máquinas que consomem muitos recursos
  - Reduzir o número de conexões de host em suas zonas
  - Reduzir o número de VDAs em suas zonas
  - Avaliar a alocação de recursos para servidores PVS
  - Aumentar a alocação de recursos para servidores PVS
  - Otimizar os Cloud Connectors para o modo LHC
- **Segurança**
  - Atualizar as versões do aplicativo Citrix Workspace que atingiram o fim da vida útil
  - Atribuir recursos a grupos de segurança
- **Otimização de custos**
  - Liberar recursos não utilizados

Esses aprimoramentos ajudam você a identificar proativamente problemas e tomar ações corretivas para manter um ambiente confiável, seguro e econômico. Para obter mais informações, consulte Citrix Advisor.

Provisionar cargas de trabalho persistentes de Amazon WorkSpaces Core Managed Instances. Anteriormente, você só podia usar o MCS para provisionar cargas de trabalho não persistentes de Amazon WorkSpaces Core Managed Instances. Com essa nova capacidade, você pode criar um catálogo persistente de Amazon WorkSpaces Core Managed Instances usando o MCS. As gravações e alterações do usuário em seus desktops são persistidas no disco do SO (volume raiz) entre diferentes inicializações de sua WorkSpaces Core Managed Instance persistente provisionada pelo MCS.

Observe que este fluxo de trabalho difere do uso do Quick Deploy para provisionar Amazon WorkSpaces Core Bundles.

Para obter mais informações, consulte Criar um catálogo de Amazon WorkSpaces Core Managed Instances.

Amazon WorkSpaces Core Managed Instances: Compartilhe imagens preparadas entre zonas de disponibilidade. Anteriormente, para criar catálogos de máquinas MCS em várias zonas de disponibilidade, você precisava de uma imagem preparada separada para cada zona de

disponibilidade. Isso aumentava sua complexidade operacional para gerenciar várias imagens preparadas e poderia levar a potenciais inconsistências no gerenciamento de imagens.

Com este recurso, você pode compartilhar uma única imagem preparada entre diferentes zonas de disponibilidade na mesma região da AWS para Amazon WorkSpaces Core Managed Instances. Isso simplifica a criação de catálogos e as atualizações de imagens, reduzindo significativamente a sobrecarga de gerenciamento. Atualmente, use comandos PowerShell para gerenciar o compartilhamento de imagens. Para obter mais informações, consulte Compartilhar imagens preparadas entre zonas de disponibilidade.

Compartilhe versões de imagens preparadas entre clusters e vCenters. Agora você pode usar o nó **Imagens** para compartilhar versões de imagens entre conexões de hospedagem no VMware. Essa implementação garante a consistência e a uniformidade das imagens em diferentes clusters ou vCenters, aprimorando a flexibilidade de implantação e a eficiência operacional. Alternativamente, você pode usar comandos PowerShell para atingir esse objetivo. Para obter mais informações, consulte Gerenciamento de imagens e Compartilhar imagens preparadas.

Crie um ambiente seguro para o tráfego gerenciado pela AWS no ambiente Amazon WorkSpaces Core. Se você tiver um proxy configurado nos Cloud Connectors, então você deve criar a conexão de host para usar o proxy para que as chamadas de API feitas pelo MCS sejam roteadas corretamente através do proxy. O MCS permite que o tráfego de rede (chamadas de API do Citrix Cloud para o hipervisor AWS) seja roteado através dos Cloud Connectors em seu ambiente Amazon WorkSpaces Core usando o Studio. Para obter mais informações, consulte Criar uma conexão usando o Studio.

Excluir VMs em modo de manutenção do pool de autoescala. Anteriormente, as VMs em modo de manutenção eram incluídas no pool de autoescala dependendo do grupo de entrega. Por exemplo, grupos de entrega de sessão única incluíam VMs em modo de manutenção no pool de autoescala, enquanto grupos de entrega de múltiplas sessões as excluíam.

Com a nova propriedade de grupo de desktop `PoolSizeExcludesMaintenanceMode`, agora você pode excluir VMs em modo de manutenção do pool de autoescala, independentemente do grupo de entrega. Se você definir a propriedade como `true`, as VMs em modo de manutenção serão excluídas do pool de autoescala. Por outro lado, se definida como `false`, elas serão incluídas. Para obter mais informações, consulte Set-BrokerDesktopGroup.

Padrão aprimorado de atribuição de usuário para maior segurança. Atualizamos o comportamento padrão ao atribuir usuários dentro de um grupo de entrega. O controle restrito agora é o padrão, garantindo melhor segurança e controle de acesso mais granular. A opção alternativa, **Permitir que qualquer usuário autenticado use recursos**, agora está claramente

marcada como **Não recomendado** e deve ser usada apenas para cenários específicos, como desktops compartilhados ou em pool para acesso amplo, ambientes de quiosque ou fins de teste. Essa alteração ajuda a reduzir riscos, ao mesmo tempo em que oferece flexibilidade quando necessário.

Para obter mais informações, consulte Configurar o escopo do usuário para uma política de acesso.

Dois novos alertas de integridade do serviço. Dois novos alertas de nível de site estão disponíveis para ajudar você a monitorar a integridade da implantação:

- Os recursos estão localizados na zona inicial.
- A verificação avançada de integridade não está habilitada no StoreFront.

Para visualizar esses alertas, clique no ícone da bandeira no canto superior direito da página inicial. Para obter mais informações, consulte Página inicial do Studio.

Gerenciamento aprimorado de pacotes de aplicativos. No Studio, agora você pode optar por remover automaticamente os pacotes que não existem mais no local de origem (agora chamado de *perfil*) ao verificar se há atualizações. Esta nova opção **Remover pacotes ausentes** no campo **Preferências** ajuda você a limpar facilmente a interface do usuário de pacotes de aplicativos, removendo entradas desatualizadas da guia **Pacotes**.

Além disso, várias guias e seções no nó Pacotes de aplicativos foram renomeadas para melhor se alinharem com o conjunto mais amplo de tipos de pacotes agora suportados no Studio:

- **Adicionar Origem** agora é **Criar perfil de descoberta**
- **Verificar atualizações de pacote** agora é **Verificar atualizações**
- **Remover origem** agora é **Excluir perfil**

Para obter mais informações, consulte Gerenciar pacotes de aplicativos.

Provisionamento entre contas no AWS EC2 usando a interface do usuário do Studio. Existem casos de uso em que os Cloud Connectors gostariam de ser colocados em uma conta AWS separada (conta de serviços compartilhados ou conta de componentes do site) com funções IAM que têm acesso entre contas (função IAM entre contas) e catálogos de máquinas provisionados por MCS em uma conta AWS secundária separada (contas de cargas de trabalho), sem a necessidade de Cloud Connectors adicionais nas contas separadas. Tal modelo de implantação já é suportado usando SDK do Powershell, e agora também é suportado usando a interface do usuário do Studio.

Configuração de proxy aprimorada para conexões de host AWS EC2. Anteriormente, o MCS não conseguia ler o valor do proxy do sistema configurado por você no Cloud Connector para configurar um proxy do sistema para uma conexão de host AWS. Com este aprimoramento, a conexão de host AWS agora pode ler o valor do proxy do sistema WinHTTP que é configurado durante a instalação do Cloud Connector se você definir a propriedade personalizada `UseSystemProxyForHypervisorTrafficOnConnectors` como `true` ao criar ou atualizar uma conexão de host usando o PowerShell. Este aprimoramento, portanto:

- Permite que o cliente AWS leia os valores do proxy, possibilitando chamadas de API adequadas através do proxy, o que é essencial para a comunicação pela internet.
- Reduz a necessidade de configurar manualmente os valores do servidor proxy e da porta via CLI.

Para obter mais informações, consulte Configuração de Proxy Aprimorada para conexão de host AWS.

Suporte a seleção múltipla para entidades-chave usando o operador “IN”. Este aprimoramento introduz a capacidade de selecionar múltiplos valores para campos de filtro chave, como usuários, máquinas e grupos de entrega, utilizando um operador "IN".

Setembro de 2025

Recursos novos e aprimorados

Suporte para o uso de instâncias Spot do AWS EC2. Com este recurso, você pode criar um catálogo de máquinas MCS de instâncias Spot (somente solicitação persistente) no ambiente de virtualização da AWS usando o fluxo de trabalho de perfil de máquina.

Em comparação com as instâncias sob demanda, as instâncias Spot oferecem economia de custos de até 90%. No entanto, as instâncias Spot podem ser interrompidas pelo Amazon EC2 se a capacidade se tornar indisponível, tornando-as adequadas apenas para aplicativos e desktops não críticos.

Além disso, com este recurso, você pode usar instâncias Spot como SKUs de backup.

Para obter mais informações, consulte Criar um catálogo usando instâncias Spot da AWS.

Acesso ao Studio com escopo para administradores de locatários CSP (Pré-visualização). Como um Provedor de Serviços Citrix (CSP), agora você pode conceder aos seus administradores de locatários acesso a uma versão leve do console do DaaS Studio diretamente de seu console do Citrix Cloud.

Em vez de serem bloqueados ao selecionar Gerenciar DaaS, os administradores de locatários agora são levados a uma visualização do Studio com escopo, onde podem gerenciar seus próprios objetos — como catálogos e grupos de entrega — com base em domínio federado e permissões baseadas em função. Objetos sem escopo ou globais, como Zonas e Tags, são ocultados para manter o isolamento do locatário e fornecer uma experiência de autoatendimento segura e simplificada.

Para obter mais informações, consulte Administração de serviço de locatário.

Conexão de Solução de Problemas do Citrix. O recurso Conexão de Solução de Problemas do Citrix foi projetado para capacitar os usuários finais a solucionar problemas potenciais de falhas de inicialização de desktop ou aplicativo de forma eficaz. Este aprimoramento visa fornecer aos usuários diagnósticos claros, recomendações potenciais e a capacidade de executar correções com um simples clique. Para obter mais informações, consulte Conexão de Solução de Problemas do Citrix.

Melhoria da multisseleção no nó de Pesquisa. Atualizamos o nó de **Pesquisa** com um layout de tabela mais intuitivo. Essa alteração permite que você:

- Selecione vários itens usando caixas de seleção em cada linha, tornando a experiência mais intuitiva.
- Selecione todos os itens na página atual usando a caixa de seleção no cabeçalho da coluna.

Embora a multisseleção e a seleção em nível de página não sejam novas (anteriormente feitas usando atalhos de teclado), este aprimoramento melhora muito a acessibilidade e a usabilidade, e estabelece as bases para o suporte futuro à multisseleção entre páginas.

Detalhes de reconexão automática de sessão na visualização Filtros e na guia Desempenho da Sessão. Agora você pode visualizar os detalhes de reconexão automática de sessão tanto na guia **Filtros** > **Sessões** quanto na guia **Desempenho da Sessão**. Este aprimoramento permite que você acesse e analise rapidamente o número de reconexões automáticas em uma sessão.

Visualização de Filtros:

Para exibir a nova coluna de Reconexão Automática de Sessão, vá para **Escolher Colunas** e selecione **Reconexão Automática de Sessão** na guia **Filtros** > **Sessões**.

Uma análise detalhada fornece informações adicionais, como Confiabilidade da Sessão ou Reconexão Automática do Cliente, carimbos de data/hora, IP do Endpoint e Nome do Endpoint da máquina onde o aplicativo Citrix Workspace está instalado. Essas informações estavam

anteriormente disponíveis na guia Tendências. Para obter mais informações, consulte a página Tendências históricas.

Guia Desempenho da Sessão:

Agora você pode visualizar os detalhes de reconexão automática da sessão na guia **Últimas 48 horas** da guia **Desempenho da Sessão**.

O gráfico exibe o número de Reconexões Totais de Sessão, Reconexões Automáticas de Cliente e Reconexões de Confiabilidade da Sessão.

As informações de reconexão automática ajudam você a visualizar e solucionar problemas de conexões de rede com interrupções e analisar redes para uma experiência perfeita.

Definições aprimoradas de medições de ICA RTT e latência de rede no Monitor. As definições e os métodos de medição para o Tempo de Ida e Volta (RTT) do ICA e a Latência da Rede no Director foram aprimorados. Esta atualização altera os contadores subjacentes e o intervalo de amostragem para essas métricas. Essas melhorias abordam limitações anteriores na forma como as métricas eram relatadas. Agora você obtém insights mais precisos e confiáveis para monitorar a experiência do usuário em ambientes Citrix.

Suporte para gerenciamento de imagens em ambientes Red Hat OpenShift. A funcionalidade de gerenciamento de imagens agora está geralmente disponível para ambientes de virtualização OpenShift. Você pode usar o nó **Imagens** para criar definições de imagem, versões e catálogos de máquinas MCS. Essa implementação reduz significativamente os custos de armazenamento e tempo, e simplifica o processo de implantação de VM e atualização de imagem. Você também pode usar comandos PowerShell para atingir esse objetivo. Para obter informações, consulte Criar um catálogo de máquinas de imagem preparada no Red Hat OpenShift.

Suporte para criação de catálogos Red Hat OpenShift usando perfil de máquina. Com este recurso, usando o Studio, agora você pode criar um catálogo Red Hat OpenShift no MCS usando um perfil de máquina. A entrada do perfil da máquina é uma VM existente. A criação de um catálogo usando um perfil de máquina permite que as VMs no catálogo herdem propriedades de hardware, como contagem de CPU e tamanho de memória. Para obter informações, consulte Criar um catálogo Red Hat OpenShift.

Gerenciando versões de imagem preparadas no XenServer. A funcionalidade de gerenciamento de imagens agora está geralmente disponível para ambientes de virtualização XenServer. Você pode usar o nó **Imagens** para criar várias versões de imagem e aplicar ou atualizar para vários catálogos de máquinas. Essa implementação reduz significativamente os custos de armazenamento e tempo, e simplifica o processo de implantação de VM e atualização

de imagem. Você também pode usar comandos PowerShell para atingir esse objetivo. Para obter mais informações, consulte Criar um catálogo de máquinas de imagem preparada no XenServer.

Melhore a confiabilidade da atualização com uma reinicialização do VDA pré-atualização. O Serviço de Atualização do VDA agora oferece a capacidade de reiniciar os VDAs antes do início da atualização. Isso ajuda a melhorar as taxas de sucesso da atualização, começando de um estado de sistema estável e evitando problemas causados por reinicializações pendentes. Para obter mais informações, consulte Atualizar VDAs.

Integração do Secure Private Access no Web Studio A integração do Secure Private Access (SPA) com o Web Studio foi aprimorada. Os administradores da sua organização agora podem abrir o console do SPA diretamente da navegação esquerda no Web Studio.

Agosto de 2025

Recursos novos e aprimorados

Suporte a seleção múltipla para grupos de entrega. Os menus suspensos de **Grupo de Entrega** nas páginas **Sessões** e **Desempenho de Logon**, na guia **Tendências**, foram aprimorados com:

- Pesquisar nomes de grupos de entrega usando entrada de texto
- Selecionar múltiplos grupos de entrega (até 15) para análise abrangente

Este aprimoramento melhora a usabilidade e permite um monitoramento e comparação mais eficientes entre vários grupos de entrega simultaneamente.

Compartilhe versões de imagem preparadas entre assinaturas e locatários no Azure. Agora você pode usar o nó **Imagens** para compartilhar versões de imagem entre conexões de hospedagem no Azure. Esta implementação garante a consistência e uniformidade das imagens entre diferentes assinaturas ou locatários, aumentando a flexibilidade de implantação e a eficiência operacional. Você também pode usar comandos PowerShell para atingir esse objetivo. Para obter mais informações, consulte Gerenciamento de Imagens.

Tratamento aprimorado de alertas de balanceamento de carga vertical e horizontal. Anteriormente, quando você definia `UseVerticalScalingForRdsLaunches` como true e configurava a política “Número máximo de sessões” no Studio, as máquinas passavam para o estado de “Capacidade máxima”. O Director acionava alertas para “Capacidade máxima” independentemente de o limite ter sido atingido devido ao balanceamento de carga vertical ou horizontal. Não havia como distinguir entre balanceamento de carga vertical e horizontal ao encontrar erros específicos, como "Carga Máxima Atingida". Isso causava alertas desnecessários

para o comportamento esperado em cenários de escalonamento vertical, desperdiçando seu tempo e criando confusão.

Agora, quando o balanceamento de carga vertical está ativo e uma máquina atinge seu limite de sessão, ela passa para um novo estado: “Capacidade máxima para escalonamento vertical”. O Director não gera mais alertas para este novo estado. Os alertas são acionados apenas para “Capacidade máxima” em cenários de escalonamento horizontal. Você pode visualizar o novo estado nas páginas **Filtros** e **Relatórios personalizados**, facilitando a distinção entre condições esperadas e excepcionais. Este aprimoramento ajuda você a evitar alertas desnecessários e a se concentrar em problemas reais, otimizando o monitoramento e a solução de problemas. Isso se aplica quando você configura `UseVerticalScalingForRdsLaunches` usando Set-BrokerSite e define a política “Número máximo de sessões” no Studio.

Alertas de saúde do Connector Appliance. Anteriormente, a criação e o gerenciamento de alertas para o Connector Appliance não estavam disponíveis. Com esta versão, você pode criar e gerenciar alertas para o Connector Appliance. Este recurso permite que os administradores monitorem a saúde dos Connector Appliances usando uma única visualização de painel e configurem alertas proativamente.

Você pode configurar alertas em Políticas de Alerta Avançadas para a saúde/conectividade e utilização de recursos dos Connector Appliances. Defina a gravidade e os escopos para que os administradores recebam alertas detalhados de acordo com a configuração do alerta. Para obter mais informações, consulte Métricas de saúde do Connector Appliance.

Coleta aprimorada de métricas de rede para solução de problemas de sessão. As métricas de rede são críticas para a solução de problemas de sessão Citrix porque o desempenho e a estabilidade da sessão dependem muito das condições da rede subjacente. Ao contrário dos aplicativos locais, as sessões Citrix transmitem experiências interativas de desktop ou aplicativo por uma rede, o que significa que qualquer instabilidade na rede impacta diretamente o desempenho do usuário.

Use as políticas no Citrix Studio para habilitar ou desabilitar a coleta de métricas de rede específicas com base em seus requisitos. As políticas fornecem aos administradores Citrix controles granulares para relatar métricas em conformidade com os requisitos de conformidade. Para obter mais informações, consulte a documentação Métricas de rede.

Observabilidade para VDA multi-sessão. O recurso de observabilidade para VDA multi-sessão aprimora os recursos de monitoramento e solução de problemas para sessões de Secure Private Access em um ambiente VDA multiusuário. Este recurso capacita os Administradores de Helpdesk

Citrix a monitorar sessões de Secure Private Access, solucionar problemas e obter insights sobre inicializações de aplicativos e transações de usuários no caso de um VDA multi-sessão.

Principais recursos:

- Observabilidade aprimorada: Os administradores podem monitorar sessões de Secure Private Access, incluindo inicializações de aplicativos e enumerações, dentro da interface do Citrix Director. Isso inclui visualizações detalhadas de problemas de enumeração e inicialização de aplicativos.
- Rastreamento de contexto do usuário: O recurso mantém o contexto do usuário para aplicativos acessados em um ambiente VDA compartilhado, garantindo visibilidade precisa dos dados da sessão para cada usuário.
- Error insights: Captura e exibe falhas de Single Sign-On (SSO), códigos de erro (por exemplo, 6003, 6007) e etapas de solução de problemas para resolver problemas.
- Pesquisa de sessão: Os administradores podem pesquisar sessões, aplicativos e transações de usuário usando o mesmo fluxo de trabalho que para sessões e aplicativos VDI.
- Navegação entre sessões: Permite a navegação entre sessões do Secure Private Access e sessões VDA para uma solução de problemas simplificada.

Para obter mais informações, consulte Observabilidade para VDA multissessão.

Agendamento personalizado para feriados. O Autoscale™ agora permite que você crie agendamentos personalizados para desligar VMs não utilizadas em um grupo de entrega em dias específicos, como feriados, para reduzir o consumo desnecessário de recursos.

Para criar agendamentos personalizados:

1. No Studio, vá para **Delivery Groups**. Clique com o botão direito do mouse em um grupo de entrega e selecione **Manage Autoscale**.
2. Na página **Schedule**, clique em **Create schedule**.

Para obter mais informações sobre como criar agendamentos personalizados para feriados, consulte Criar agendamentos de feriados personalizados usando o Studio.

Suporte para gerenciamento de imagens com VMs confidenciais do Azure usando a interface do usuário do Studio. Agora você pode usar o nó **Imagens** para preparar e gerenciar imagens compatíveis com VMs confidenciais do Azure. Você também pode usar comandos PowerShell para atingir esse objetivo. Para obter mais informações, consulte:

- VMs confidenciais do Azure

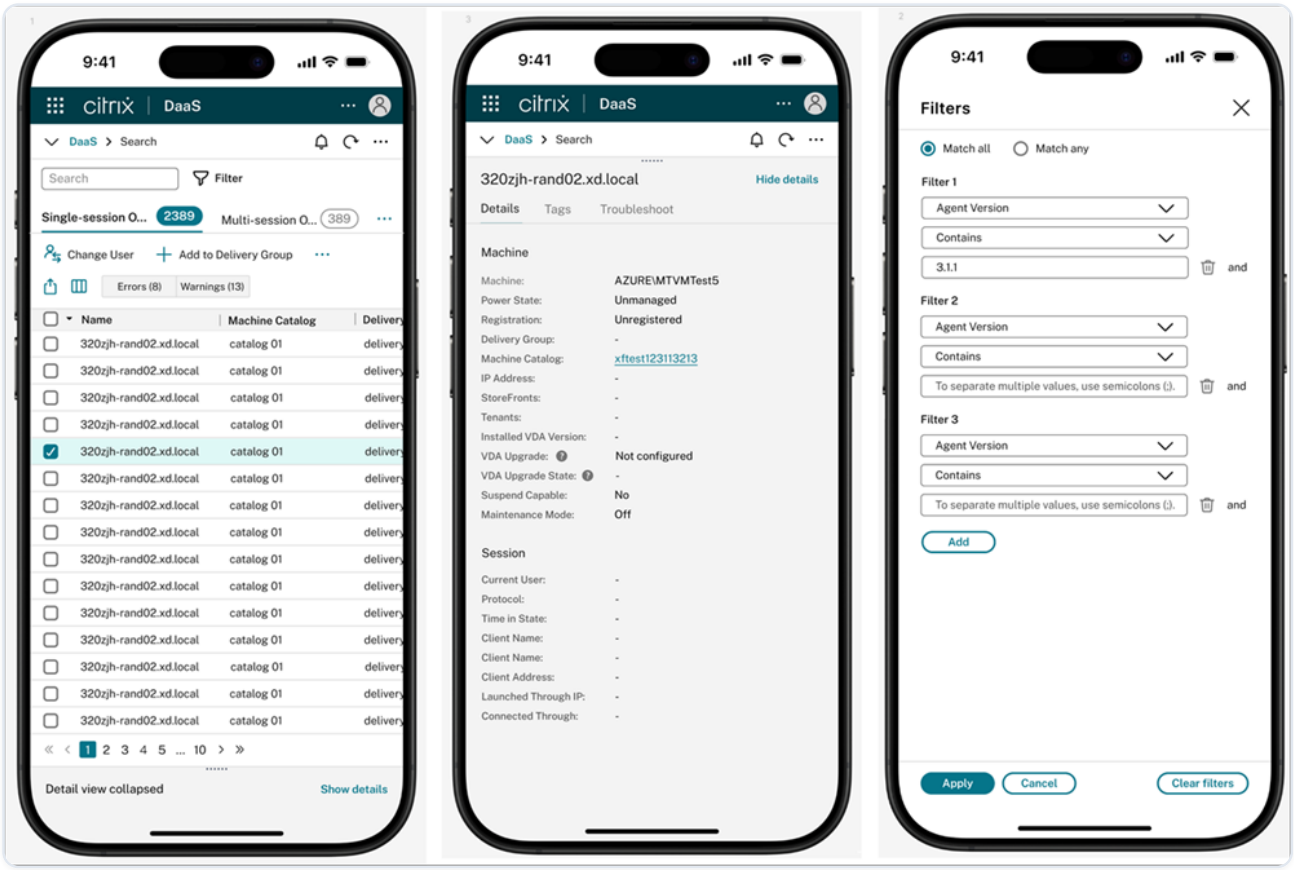
- Criar uma definição de imagem e versão inicial da imagem

Experiência móvel aprimorada para tarefas DaaS críticas em trânsito. Agora você pode gerenciar o Citrix DaaS com mais facilidade a partir do seu dispositivo móvel. A experiência atualizada é otimizada para telas menores, tornando mais fácil acessar o Studio de um dispositivo móvel quando um desktop não está disponível. Seja respondendo a um alerta ou verificando rapidamente uma configuração incorreta, você pode agir imediatamente — sem precisar esperar até voltar à sua mesa.

A interface móvel oferece acessibilidade aprimorada e é projetada para interações amigáveis ao toque. Os layouts e a funcionalidade podem diferir ligeiramente da experiência de desktop para melhor se adequar aos fluxos de trabalho móveis.

Com um layout responsivo e navegação simplificada, você pode:

- Monitore a saúde do DaaS rapidamente
- Visualize detalhes para catálogos de máquinas e grupos de entrega
- Realize ações importantes, como reiniciar máquinas ou desabilitar grupos de entrega



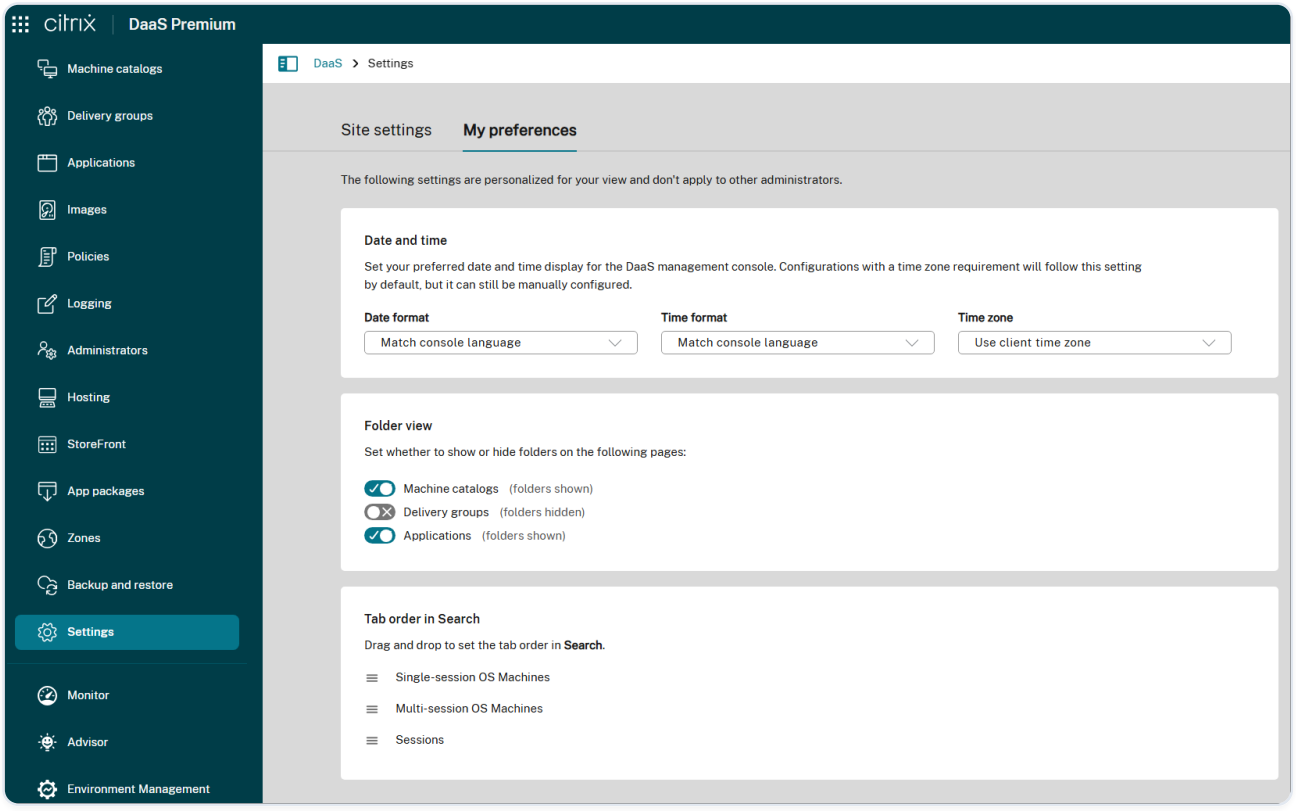
Personalize sua visualização do Studio com as configurações de Minhas preferências. Uma nova guia **Minhas preferências** agora está disponível no nó **Configurações**. As configurações nesta guia permitem que você personalize sua interface do Studio para atender às suas

preferências. Essas configurações se aplicam apenas à sua conta e não afetam outros administradores.

Você pode configurar as seguintes opções:

- **Data e hora**: Defina seu fuso horário padrão, formato de data e formato de hora. Essas configurações são usadas em todo o Studio para exibições relacionadas ao tempo, como reinícios agendados e dimensionamento automático.
- **Visualização de pasta:** Escolha se deseja mostrar ou ocultar a visualização de pasta nos nós **Catálogos de Máquinas**, **Grupos de Entrega** e **Aplicativos**.
- **Ordem das guias na Pesquisa**: Personalize a ordem das guias dentro do nó **Pesquisa**.

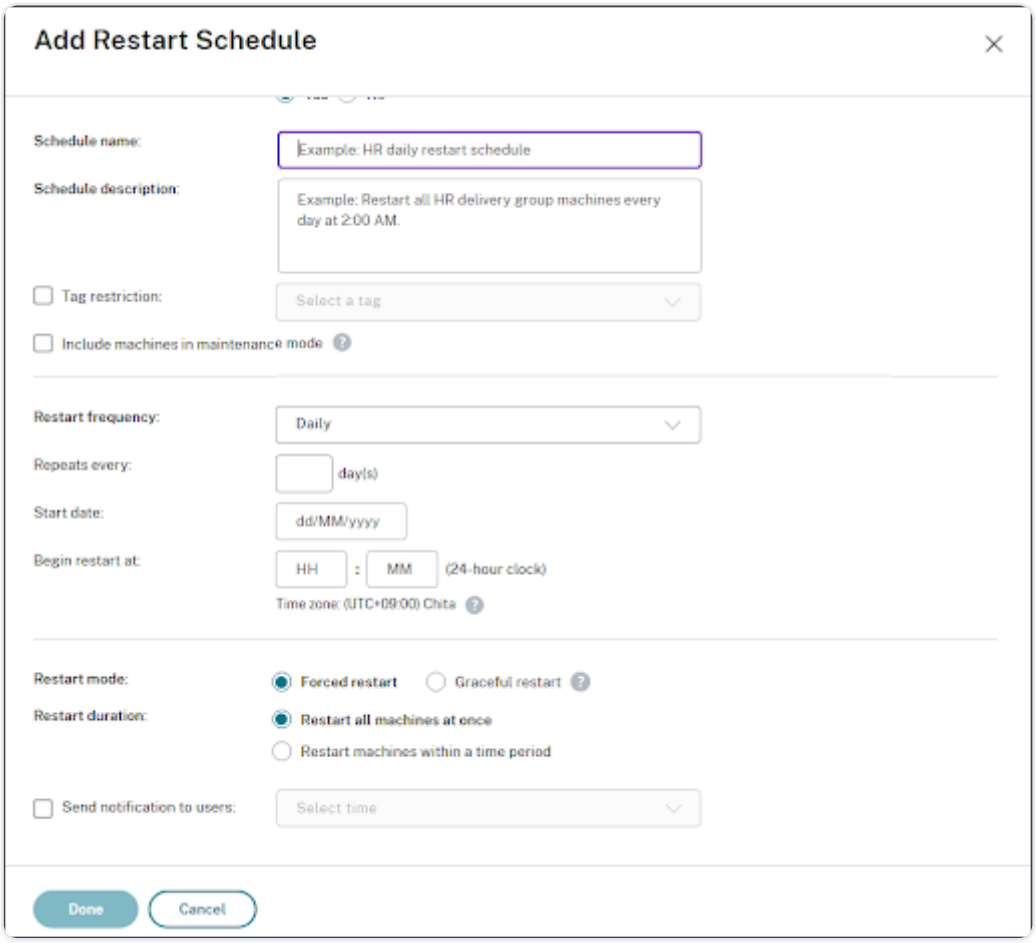
Para obter mais informações, consulte Gerenciar preferências pessoais no Studio



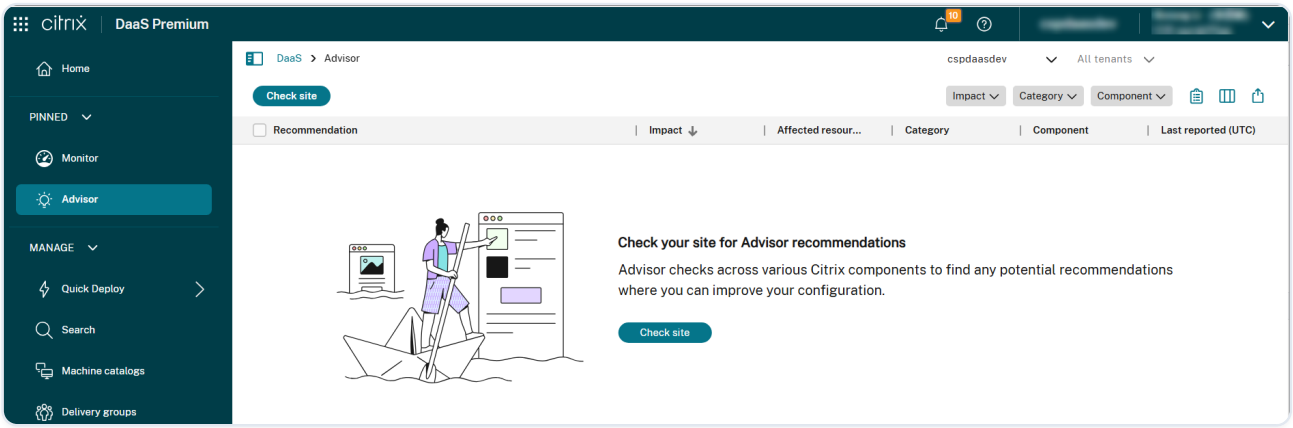
Interface de usuário de reinício aprimorada para controle e personalização mais claros. Aprimoramos a interface de usuário de agendamento de reinício para tornar os modos de reinício mais claros e personalizáveis. Agora você pode distinguir facilmente entre *reinício gracioso* e *reinício forçado*, e configurar durações de reinício personalizadas para atender às suas necessidades.

Para ajudá-lo a fazer escolhas informadas, também adicionamos dicas de ferramentas que explicam as principais opções — como o reinício forçado pode reiniciar máquinas à força, mesmo que as sessões não respondam.

Para obter mais informações, consulte Gerenciar grupos de entrega.



Citrix Advisor: Insights proativos e otimização para sua implantação DaaS. O Citrix Advisor é um serviço que ajuda você a otimizar a implantação DaaS e aprimorar sua saúde e prontidão gerais. Ele automatiza verificações de ambiente e oferece recomendações acionáveis, capacitando você a identificar proativamente problemas de configuração, ineficiências, desperdício de recursos, desvios das melhores práticas e muito mais.



Com o Advisor, você pode:

- **Identificar e resolver problemas proativamente:** Detectar problemas potenciais, desvio de configuração e desvios das melhores práticas antes que eles afetem os usuários, interrompam as operações comerciais ou comprometam a segurança.
- **Otimizar o desempenho e a estabilidade do ambiente:** Ajustar configurações, otimizar a alocação de recursos e implementar as melhores práticas para aprimorar a estabilidade, segurança e desempenho de suas implantações Citrix.
- **Simplificar operações e reduzir a sobrecarga:** Automatizar verificações de rotina, simplificar tarefas de remediação complexas e receber assistência guiada, reduzindo assim a sobrecarga operacional e liberando recursos administrativos.
- **Otimizar custos e utilização de recursos:** Identificar áreas de gastos excessivos, descobrir oportunidades de otimização de recursos e garantir a utilização eficiente das tecnologias Citrix para minimizar o custo total de propriedade.
- **Manter a conformidade e a adesão às melhores práticas:** Garantir que as implantações Citrix sigam as melhores práticas da Citrix, padrões de segurança e regulamentações do setor, reduzindo riscos e melhorando a governança geral.
- **Simplificar tarefas complexas:** Simplificar tarefas administrativas para suportar um ambiente saudável e otimizado.

Para obter mais informações, consulte Citrix Advisor.

Julho de 2025

Recursos novos e aprimorados

Resumo de custos. A página **Resumo de custos** fornece um resumo abrangente das despesas associadas à execução do ambiente Citrix. Com este aprimoramento, você obtém visibilidade sobre o seguinte:

- O custo total por usuário
- Custo de entrega de virtualização pelos provedores de carga de trabalho escolhidos, tipos de desktop e conjuntos de séries de VM

Esta página oferece:

- Visão sobre o custo de entrega de um aplicativo ou desktop virtualizado a um usuário O valor economizado
- Informações sobre custos e economias categorizadas por
    - Provedor de plataforma

- Tipo de SO
- Tipo de desktop
- Série de VM

> **Nota:**
>
> A página **Resumo de custos** está disponível somente se o site estiver em execução por pelo menos 15 dias em um mês.
>
> Para obter mais informações, consulte a página Resumo de custos.

Provisionamento entre contas no AWS EC2 usando PowerShell. Existem casos de uso em que os Cloud Connectors gostariam de ser colocados em uma conta AWS separada (conta de serviços compartilhados ou conta de componentes do site) com funções IAM que têm acesso entre contas (função IAM entre contas) e catálogos de máquinas provisionados por MCS em uma conta AWS secundária separada (contas de cargas de trabalho), sem a necessidade de Cloud Connectors adicionais nas contas separadas. Para suportar tais cenários, este recurso usa o emparelhamento de VPC e o acesso entre contas usando funções IAM para tornar o provisionamento entre diferentes contas AWS possível para empresas que gerenciam várias contas AWS.

Com o emparelhamento de VPC, você pode ter seu Cloud Connector e VMs provisionadas em diferentes regiões ou contas capazes de se comunicar entre si.

Com o acesso entre contas usando funções IAM, você permite que a conta principal (conta do Cloud Connector) assuma uma função IAM para acessar recursos da AWS na conta secundária (VMs do catálogo de máquinas).

Para obter informações detalhadas, consulte Provisionamento entre contas.

Suporte para lista de SKU de backup para VMs no AWS EC2. As nuvens públicas podem, às vezes, ficar sem capacidade para um tipo específico de instância EC2 (**SKU primário**). Se a configuração da VM primária não estiver disponível, a VM não poderá iniciar, resultando em perda de tempo e interrupção dos negócios.

Com este recurso, no ambiente de virtualização AWS, você pode fornecer uma lista de tipos de instância EC2 de backup (**SKUs de Backup** que podem ser instâncias **Sob Demanda**) usando PowerShell para os quais o MCS pode recorrer em caso de problemas relacionados à capacidade.

O MCS tenta recorrer aos tipos de instância EC2 de backup na ordem fornecida por você na lista. Caso o MCS não consiga recorrer a todos os tipos de instância EC2 de backup fornecidos, você receberá uma mensagem de erro. Este recurso é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

Para obter mais informações, consulte Lista de SKUs de backup para VMs.

Diagnóstico aprimorado de inicialização de sessão com ações recomendadas. A página atualizada de **Diagnóstico de Falha na Inicialização da Sessão** oferece uma compreensão mais aprofundada dos problemas de inicialização da sessão. Você pode encontrar a visualização dos componentes envolvidos com análise de erros e ações recomendadas. Anteriormente, apenas um painel de **Detalhes da Transação** estava disponível, que listava os componentes envolvidos e indicava os locais dos erros.

A página aprimorada agora inclui:

- Visão geral dos componentes: Esta seção exibe todos os componentes envolvidos no processo de inicialização da sessão, adaptando-se ao cenário específico e à fase de falha. Exemplos de componentes incluem Endpoint, Citrix Workspace™, Citrix DaaS, Cloud Connector, Gateway Service, VDA e StoreFront. O componente da causa raiz é claramente destacado.
- Detalhes do erro: Mensagens de erro específicas e contexto são fornecidos para rápida identificação da causa raiz.
- Logs de transação: Dados brutos de eventos de inicialização de sessão são acessíveis para solução de problemas e análise aprofundada.

Esses aprimoramentos permitem que os administradores de TI resolvam problemas de inicialização de sessão de forma mais rápida e eficiente. Para obter mais informações, consulte a documentação Diagnóstico de Inicialização de Sessão.

Integração com o Nutanix Prism Central no AHV. Agora você pode conectar o Citrix DaaS a clusters Nutanix AHV através do Nutanix Prism Central usando uma nova conexão de host, Nutanix AHV Prism Central.

Os benefícios de usar a conexão de host Nutanix AHV Prism Central são:

- Suporta catálogos de máquinas com VDAs gerenciados apenas por energia e provisionados por MCS.
- Permite o compartilhamento de VM mestre do MCS entre clusters AHV usando a versão do modelo.

- Simplifica a confiança do certificado na conexão do host.
- Elimina a necessidade de instalar separadamente o plug-in nos Cloud Connectors.

Para obter mais informações, consulte:

- Ambientes de virtualização Nutanix
- Soluções de nuvem e parceiros Nutanix
- Conexão com Nutanix
- Conexão com soluções de nuvem e parceiros Nutanix
- Criar um catálogo Nutanix
- Gerenciar um catálogo Nutanix

Suporte para a criação de catálogos de máquinas MCS não persistentes no Amazon Workspaces Core. O MCS agora se integrou ao Amazon Workspaces Core para provisionar catálogos de máquinas MCS não persistentes na conta AWS do cliente. Para uma comparação de como essa nova integração se compara ao MCS para AWS EC2 e Quick Deploy para Amazon WorkSpaces Core Bundles e como configurar o local do recurso, consulte Ambientes de virtualização AWS.

Com este recurso:

- Você pode criar uma conexão de host com instâncias gerenciadas do Amazon WorkSpaces Core.
- Criar uma imagem preparada e usar a imagem preparada e o perfil da máquina para criar um catálogo de máquinas MCS não persistente.

Personalize ícones de desktop em todas as plataformas usando o Studio. O Studio agora permite personalizar ícones de desktop para qualquer desktop de sua escolha. Anteriormente, todos os desktops usavam o ícone padrão e você não podia alterá-lo no Studio. Agora você pode:

- Carregar ícones e usá-los para desktops ou aplicativos
- Alterar o ícone para desktops individuais
- Selecionar entre ícones integrados para os desktops de sua escolha

Para obter mais informações, consulte Criar grupos de entrega e Gerenciar grupos de entrega.

Studio: Suporte para controle mais granular sobre políticas de acesso em grupos de entrega. Anteriormente, você podia aplicar políticas de acesso a usuários específicos apenas usando PowerShell ou APIs REST. Agora, você pode atingir esse objetivo diretamente no Studio.

Este aprimoramento oferece mais flexibilidade na definição de diferentes condições de acesso para vários usuários ou grupos de usuários, alcançando um controle de acesso mais granular. Para obter mais informações, consulte Configurar escopo de usuário para uma política de acesso.

Além disso, melhoramos a compatibilidade entre o Studio e a abordagem de PowerShell ou API REST. Anteriormente, se você configurasse políticas de acesso com escopos de usuário usando PowerShell ou APIs REST, as páginas de Usuários e Políticas de Acesso no Studio eram bloqueadas. O Studio agora oferece suporte total a esses cenários, fornecendo informações claras ou orientação da interface do usuário quando necessário.

Opção de usar proxy de sistema em Citrix Cloud™ Connectors para tráfego de API redirecionado do Azure e GCP. Com este recurso, você pode redirecionar o tráfego de internet da API do Azure e GCP nos Citrix Cloud Connectors através do proxy do sistema. Isso ajuda a rotear todo o tráfego externo através de um proxy não transparente.

Para obter informações sobre como habilitar o proxy, consulte:

- Para Azure:
  - Studio: Criar um service principal e conexão usando o Studio
  - PowerShell: Opção de usar proxy de sistema em Citrix Cloud Connectors para tráfego de API redirecionado do Azure
- Para GCP:
  - Studio: Adicionar uma conexão
  - PowerShell: Opção de usar proxy de sistema em Citrix Cloud Connectors para tráfego redirecionado do GCP

Compartilhar imagem preparada criptografada entre assinaturas e locatários para Azure. As imagens da Azure Compute Gallery (ACG) podem ser criptografadas com um Conjunto de Criptografia de Disco (DES). Com este recurso, você pode compartilhar uma imagem preparada criptografada entre assinaturas e locatários. Você pode, então, criar um catálogo de máquinas no recurso onde a imagem preparada criptografada é compartilhada. Para obter mais informações, consulte Compartilhar imagens preparadas criptografadas entre regiões, assinaturas e locatários.

Adicionar notas ao atribuir imagens preparadas. Com este recurso, agora você pode adicionar notas personalizadas usando o Studio e o PowerShell ao criar ou atualizar um catálogo MCS com uma imagem preparada. O MCS mantém um registro de todas as atribuições de imagens preparadas. Isso ajuda você a:

- Recuperar o histórico de atribuições de todas as imagens preparadas atribuídas a um catálogo.
- Reverter rapidamente um catálogo de máquinas para uma imagem preparada atribuída anteriormente usando a ação **Usar atribuição de imagem anterior para reversão rápida**. Basta selecionar uma versão da lista de histórico para uma reversão rápida e informada. Para obter informações sobre como reverter, consulte Atualizar um catálogo de máquinas com uma imagem preparada diferente.

Este recurso é aplicável a ambientes Azure e VMware

Para obter informações sobre como criar um catálogo com imagens preparadas, consulte:

- Criar um catálogo de máquinas com imagem preparada no Azure
- Criar um catálogo de máquinas com imagem preparada no VMware

Para obter informações sobre como atualizar um catálogo com imagens preparadas, consulte Gerenciar catálogos de máquinas com imagem preparada.

Suporte para integração do Azure Arc em todos os hipervisores locais. O Azure Arc permite que as organizações gerenciem recursos como VMs hospedadas em qualquer lugar como se estivessem sendo executadas no Azure. Com o Azure Arc, você pode usar serviços do Azure, como o Azure Monitor, para visibilidade abrangente e gerenciamento proativo dos recursos.

Com este recurso, agora você pode habilitar a integração do Azure Arc para um catálogo de máquinas MCS usando comandos do PowerShell. Uma vez integradas, as VMs podem ser gerenciadas a partir do portal do Azure para realizar operações como gerenciamento de energia, adicionar ou remover extensões, atribuir políticas e habilitar o Azure Monitor nas VMs habilitadas para Arc por meio da política interna do Azure.

Atualmente, este recurso é aplicável a todos os hipervisores locais da Citrix: VMware, Nutanix e SCVMM.

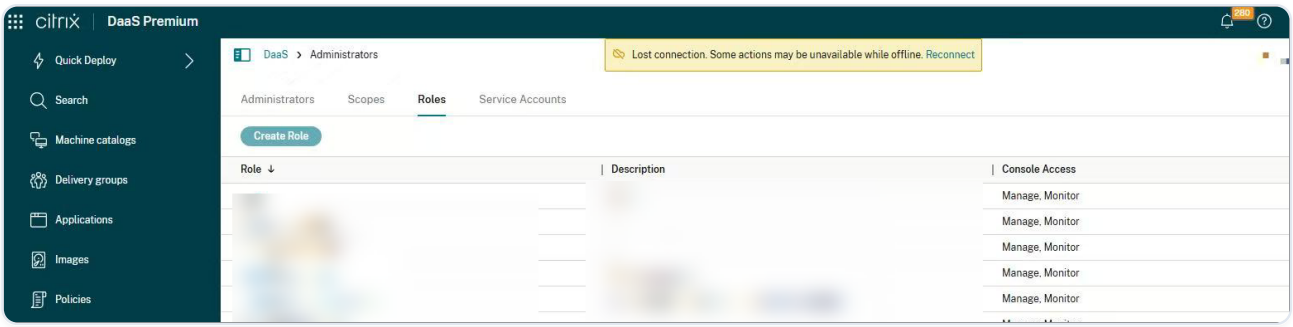
Para obter mais informações, consulte Integrar VMs ao Azure Arc.

Migração de discos não gerenciados para gerenciados no Azure. Em September 30, 2025, o Azure desativará oficialmente os discos não gerenciados (ou seja, VHDs). Após esta data, você não poderá mais iniciar VMs do Azure que usam discos não gerenciados. Com este recurso, você pode migrar suas VMs do Azure provisionadas por MCS de discos não gerenciados para gerenciados por meio do Citrix.

A migração se aplica a catálogos de máquinas persistentes e não persistentes, suportando VMs sob demanda e legadas. Isso garante uma integração perfeita com os padrões atualizados de gerenciamento de disco do Azure e evita interrupções de serviço devido à desativação de discos não gerenciados. Para obter mais informações, consulte Migrar de discos não gerenciados para gerenciados.

Suporte para gerenciamento de imagens com VMs confidenciais do Azure. Agora você pode preparar e gerenciar imagens compatíveis com VMs confidenciais do Azure. Essas imagens garantem que as VMs provisionadas a partir desses catálogos de máquinas MCS sejam criptografadas na memória e protegidas durante o uso. Para obter mais informações sobre gerenciamento de imagens, consulte Gerenciamento de imagens.

Modo sempre ativo do Studio. O Web Studio agora apresenta o modo sempre ativo para aumentar a resiliência e reduzir o tempo de inatividade durante falhas de infraestrutura. Neste modo somente leitura, você pode visualizar e monitorar com segurança seu ambiente Citrix DaaS mesmo durante interrupções de serviço, ajudando a manter a continuidade operacional. O modo sempre ativo está disponível em todos os nós MANAGE, exceto Quick Deploy. Para obter mais informações, consulte esta postagem do blog.



Studio: Suporte para gerenciamento de grupos de segurança do Azure AD usando contas de serviço. No Studio, agora você pode usar contas de serviço do Azure AD para configurar e gerenciar grupos de segurança dinâmicos para VMs. Anteriormente, a configuração de grupos de segurança do Azure AD exigia a inserção manual de credenciais. Esta atualização permite que você use uma conta de serviço pré-configurada para realizar o gerenciamento de grupos de segurança sem interação do usuário, simplificando o processo e aprimorando a segurança.

Para obter mais informações, consulte Contas de serviço do Azure AD e Criar um catálogo do Microsoft Azure.

Migrar catálogos MCS provisionados existentes para catálogo de máquinas de imagem preparada. Com este recurso, você pode converter um catálogo MCS existente provisionado a partir de uma imagem mestre para um catálogo usando uma imagem preparada. Para obter informações sobre imagem preparada, consulte Gerenciamento de imagens.

No entanto, você não pode reverter para o catálogo herdado após a migração. Atualmente, este recurso é aplicável a ambientes de virtualização Azure e VMware. Para obter informações sobre as etapas para migrar, consulte Migrar catálogos MCS provisionados existentes para catálogo de máquinas de imagem preparada.

Exibir SKUs NVMe v6 para uso de OSDisk efêmero. Agora você tem a opção de armazenar um disco de SO efêmero em um disco NVMe usando o Studio. Para obter informações, consulte Discos efêmeros do Azure.

Duração atualizada do estado HA Pendente. A duração do estado HA Pendente, quando os Cloud Connectors determinam se há necessidade de entrar no modo LHC, foi estendida de 60 para 90 segundos. Para obter informações sobre os estados do LHC, consulte Estados do Cache de Host Local.

Junho de 2025

Recursos novos e aprimorados

Suporte para atribuir Políticas de Grupo Citrix a usuários do Microsoft Entra ID. Agora você pode atribuir Políticas de Grupo Citrix a usuários do Microsoft Entra ID (Azure AD) de vários IDPs no Studio. Este aprimoramento oferece mais flexibilidade ao aplicar políticas a grupos de usuários específicos e simplifica as implantações usando o Citrix DaaS com o Windows 365. Para obter mais informações, consulte Especificar atribuições de política.

Monitoramento dos detalhes da duração do logon do VDA. O Citrix Monitor agora inclui informações detalhadas sobre a duração do logon do VDA para fornecer visibilidade sobre o tempo necessário para fazer logon no VDA. Os seguintes itens são adicionados para visualizar os detalhes da duração do logon do VDA:

- As seguintes métricas são adicionadas à dica de ferramenta como métricas de detalhamento:
  - **Associações de arquivos AppX**: O tempo necessário para associar arquivos AppX durante a nova sessão VDA.
  - **Pacotes de carregamento AppX**: O tempo necessário para carregar os pacotes AppX durante a nova sessão VDA.

  Essas métricas são exportadas nos formatos PDF e CSV, e o gráfico também é incluído nos arquivos exportados.

- Detalhamento da etapa **Shell** na guia **Logon da Sessão**: Associações de arquivos AppX e pacotes de carregamento AppX são adicionados como um detalhamento da etapa de sessão interativa no gráfico na guia de gráfico **Logon da Sessão**.

Benefícios:

- Solução de problemas precisa: Ajuda os administradores a determinar com precisão as causas de logons lentos, que podem ser frequentemente devido ao tipo de implantação, GPOs, perfis e interação do usuário.
- Ações corretivas: Permite que os administradores tomem ações corretivas nas áreas certas, melhorando a experiência geral do usuário.

Este recurso foi projetado para melhorar a análise detalhada do logon da sessão, fornecendo uma representação mais precisa do desempenho do logon e da triagem do logon da sessão para o suporte técnico do Director.

Para obter mais informações, consulte Fases do processo de logon.

Métricas de endpoint disponíveis na guia Filtros e Relatórios Personalizados. Anteriormente, as métricas de endpoint estavam disponíveis apenas na exibição de Endpoint na seção **Detalhes do Usuário** > **Desempenho da Sessão** > **Topologia da Sessão**.

Com este aprimoramento, agora você pode visualizar as seguintes métricas de endpoint adicionais nos filtros de Conexão ou Sessão do Monitor e nos Relatórios Personalizados:

- Endereço IP público
- ISP
- Localização (País ou Cidade)
- Tipo de Workspace - aplicativo Citrix Workspace (aplicativo ou navegador)
- Tipo de acesso (via Workspace ou StoreFront)

Este aprimoramento ajuda você a fazer o seguinte:

- Você pode selecionar as métricas de endpoint como parte da seleção de colunas na guia **Filtros**.
- Você pode criar relatórios personalizados usando a opção **Consulta Personalizada**, selecionando colunas de saída como métricas de endpoint.

Descarte de alertas em massa. Este recurso visa otimizar o processo de gerenciamento de alertas para administradores, fornecendo mais flexibilidade e reduzindo a fadiga de alertas. Ele

permite que os administradores descartem alertas em massa por tempo, tipo ou categoria, facilitando o gerenciamento de alertas, especialmente durante modos de manutenção ou ao lidar com alertas de hipervisores e outros ambientes.

Ao permitir o descarte em massa de alertas, os administradores podem gerenciar sua carga de trabalho de forma mais eficiente e evitar serem sobrecarregados por um alto volume de alertas.

Para obter mais informações, consulte Descarte de alertas em massa.

Monitoramento aprimorado de métricas de rede no Citrix Monitor. O Citrix Monitor agora oferece aos administradores visibilidade incomparável do desempenho da sessão. Esse aprimoramento os capacita a identificar e resolver proativamente gargalos, otimizar aplicativos e garantir uma experiência de usuário superior.

Principais aprimoramentos:

- **Monitoramento de latência L7**: Identifique e resolva problemas de desempenho monitorando o tempo de processamento em nível de aplicativo (latência L7).
- **Novas métricas de rede**: Obtenha uma compreensão abrangente do desempenho da rede por meio de insights sobre taxa de transferência e retransmissões do lado do cliente.
- **Dados históricos**: Identifique padrões e possíveis problemas visualizando as tendências de latência dos últimos 15 minutos e 24 horas.
- **Filtragem**: Realize análises e solução de problemas direcionadas filtrando dados de latência na página **Filtros**.
- **Visualização do caminho de conexão da sessão**: Identifique e resolva rapidamente problemas de latência visualizando o caminho de conexão do usuário final para as máquinas VDA, incluindo saltos de rede e componentes.

Benefícios:

- **Visibilidade aprimorada**: Identifique rapidamente as causas raiz de experiências de sessão insatisfatórias.
- **Solução de problemas eficiente**: Otimize a solução de problemas de latência com uma visualização clara do caminho de conexão da sessão.

Métricas coletadas:

- Taxa de transferência
- Latência do Servidor L7

- Latência do Cliente L7
- Retransmissões do Lado do Cliente

> **Nota:**
>
> - Para visualizar as novas métricas, ative a política de **Telemetria de Rede** no Citrix Web Studio. Após ativar a política, os usuários devem iniciar uma nova sessão para que as alterações entrem em vigor.
> - A latência L7 é medida para sessões HDX™ estabelecidas com o aplicativo Citrix Workspace para Windows e VDA do Windows através do serviço Gateway.
> - Após iniciar uma sessão:
> - Novas métricas estão disponíveis nas seções **Topologia da Sessão** e **Últimos 15 Minutos** após uma espera de 2 minutos.
> - Dados históricos (das últimas 48 horas) estão disponíveis após aproximadamente 5 minutos devido à janela de agregação de 5 minutos.

> Com essas melhorias, o Citrix Monitor equipa os administradores com as ferramentas para otimizar proativamente o desempenho do aplicativo e oferecer uma experiência de usuário perfeita.

Para obter mais informações, consulte a documentação Visualização de Salto de Rede de Ponta a Ponta.

Suporte para plug-in OpenShift gerenciado pela Citrix. Com este recurso, a Citrix gerencia suas cargas de trabalho do Red Hat OpenShift por meio de um plug-in OpenShift gerenciado pela Citrix. Com este plug-in, você pode criar conexões de hospedagem e unidades de hospedagem para seu cluster OpenShift, criar catálogos e gerenciar o consumo de energia das máquinas no catálogo. Para obter mais informações, consulte:

- Ambientes de virtualização Red Hat OpenShift
- Conexão com o Red Hat OpenShift
- Criar um catálogo Red Hat OpenShift

Desempenho aprimorado da interface do usuário para importação de VMs do AWS. Aprimoramos o desempenho da interface do usuário do Studio otimizando o processo de

importação de VMs para o Citrix DaaS do AWS. Para evitar timeouts causados pela busca de um grande número de AMIs, o Studio não recupera mais AMIs durante este processo.

Conta de serviço para roteamento de tráfego de identidade do Azure AD. Usando este recurso, você pode criar e modificar uma conta de serviço do Azure AD para rotear o tráfego de identidade do Azure AD do Delivery Controller para o Azure AD através do Citrix Cloud Connector para aprimorar a segurança. Para obter mais informações, consulte Roteamento de gerenciamento de dispositivos Azure AD e tráfego de gerenciamento de grupos de segurança.

Suporte para atribuição de grupos de segurança por interface de rede a VMs usando o perfil de máquina na AWS. No ambiente de virtualização da AWS, agora você pode criar um catálogo de máquinas MCS onde as VMs provisionadas recebem grupos de segurança por ENI (Network Interface). Para fazer isso, use uma entrada de perfil de máquina (instância EC2 ou modelo de inicialização) que tenha diferentes grupos de segurança mapeados para ENIs distintas. Por exemplo, se a entrada do perfil de máquina tiver ENI A com SG 1 e ENI B com SG 2, as VMs provisionadas também terão ENI A com SG 1 e ENI B com SG 2.

Este recurso se aplica a:

- Catálogos persistentes e não persistentes
- Novos catálogos de máquinas
- Novas VMs provisionadas para um catálogo existente

Para obter informações, consulte Criar um catálogo de máquinas baseado em perfil de máquina usando PowerShell.

Suporte para criação de conexões de host usando o Azure Managed Identity com o Studio. Usando o Studio, agora você pode criar conexões de host com o Microsoft Azure Resource Manager usando o Azure Managed Identity. Esse método oferece uma alternativa segura e escalável ao uso de uma entidade de serviço, eliminando a necessidade de gerenciar credenciais manualmente. As identidades gerenciadas suportam a atualização automática de tokens e reduzem os riscos associados ao armazenamento e rotação de segredos. Alternativamente, você pode usar o PowerShell. Para obter mais informações, consulte Criar uma conexão de host usando o Azure Managed Identity e Gerenciar o Azure Managed Identity de uma conexão de hospedagem existente.

Modelagem de custos para cargas de trabalho do Azure. O novo recurso de modelagem de custos oferece suporte a cargas de trabalho do Azure e fornece recomendações com base nos padrões de uso. Os clientes recebem recomendações sobre se as Reservas do Azure ou o Plano de Economia são mais adequados para proporcionar a máxima economia de custos. Os clientes

de Reservas do Azure reservam um número específico de máquinas antecipadamente a um custo fixo com desconto, enquanto os planos de economia permitem que eles se comprometam com um valor em dólar para taxas com desconto. O recurso analisa os dados dos últimos 28 dias para fornecer recomendações estimadas. Esse recurso ajuda os clientes a economizar custos tomando decisões informadas sobre a alocação de recursos.

> **Nota:**
>
> Para estimativas ideais, recomenda-se usar dados de um ambiente estável nos últimos 28 dias. Evite usar dados de períodos de atividade incomum, como férias ou picos repentinos de uso. Espere até que seu uso retorne aos níveis de linha de base antes de seguir essas recomendações.

> **Benefícios:**

- Fornece recomendações personalizadas de economia de custos.
- Suporta planos de reserva e de economia.
- Analisa dados de uso recentes para insights precisos.
- Ajuda a otimizar a alocação de recursos e reduzir despesas.
- Oferece flexibilidade na seleção de grupos de entrega, tags, séries de VM e regiões.

Para obter mais informações, consulte a página Modelagem de custos.

Visualize e filtre máquinas por estado de atualização do VDA no Studio. O Studio agora inclui **Estado de Atualização do VDA** como uma coluna nos nós **Pesquisa** e **Catálogos de Máquinas**. Esta coluna mostra o status das atualizações agendadas do VDA — por exemplo, se uma atualização foi bem-sucedida. Você também pode filtrar máquinas com base no estado de atualização do VDA, facilitando o rastreamento e o gerenciamento das atualizações do VDA em sua implantação.

Para obter mais informações sobre esta coluna, consulte Ações e colunas da máquina.

Opção para estender o monitoramento da otimização HDX além do Microsoft Teams. O Citrix Monitor agora adiciona uma opção para estender o monitoramento da otimização HDX além do Microsoft Teams. Anteriormente, apenas o Microsoft Teams estava disponível para monitoramento da otimização HDX, mostrando se estava otimizado ou não na tela **Topologia da Sessão**. Com este novo recurso, em vez de **Microsoft Teams**, um novo parâmetro chamado **Comunicações**

em tempo real é adicionado na tela **Topologia da Sessão**. Atualmente, apenas o Microsoft Teams é monitorado para o status de otimização HDX. No entanto, este recurso oferece a possibilidade de adicionar mais softwares para monitoramento além do Microsoft Teams no futuro. Este recurso permite que os administradores monitorem e solucionem problemas de aplicativos com e sem otimizações HDX, proporcionando uma melhor experiência ao usuário.

Você pode clicar em **Ver detalhes** ao lado do aplicativo para visualizar informações adicionais, como categorização em Otimização de Terceiros e Otimização HDX. Para o Microsoft Teams Slims core, ele faz parte da otimização de terceiros. Se não fizer parte da otimização de terceiros, então é otimizado para HDX.

Principais recursos e benefícios:

- **Monitoramento abrangente**: Monitore e solucione problemas de aplicativos otimizados e não otimizados para HDX.
- **Insights detalhados**: Visualize informações detalhadas sobre o status de otimização dos aplicativos.

> **Nota:**
>
> - Para usar este novo recurso, certifique-se de que você está usando o aplicativo Citrix Workspace para Windows versão 2503 e o VDA versão 2503.
> - Para usar o Microsoft Teams Slims core, você deve instalar o gerenciador de plug-ins no endpoint, configurar a lista de permissões para o canal virtual e garantir que o canal virtual esteja aberto. Este recurso é apenas para sessões HDX.

> Para obter mais informações, consulte Detalhes da otimização HDX.

Novas métricas no painel do Monitor. O painel do Citrix Monitor é enriquecido com as duas métricas a seguir para fornecer informações valiosas aos administradores:

- **Total de usuários conectados**: Mostra o número de usuários que tiveram pelo menos uma conexão nas últimas 24 horas e nos últimos 7 dias. Ajuda os administradores a apresentar tendências de adoção aos seus executivos.
- **Versões do aplicativo Citrix Workspace encontradas em seu ambiente**: Fornece uma visão geral das versões do aplicativo Citrix Workspace usadas em toda a organização. Ajuda a

unificar as versões mostrando quantos dispositivos estão usando versões diferentes. Você pode selecionar **Todos** ou um SO específico na lista suspensa **Plataforma**.

Este recurso fornece pontos de dados essenciais para os administradores monitorarem e gerenciarem seus ambientes de forma eficaz.

Para obter mais informações, consulte a página Análise do Site.

Aprimoramentos na página Economia de custos. Os seguintes aprimoramentos foram feitos na página Economia de custos para fornecer maior flexibilidade e percepção ao gerenciar custos:

- **Opção de suporte para filtro de provedor de serviços**: Agora você pode filtrar por provedores de serviços. Se um site tiver cargas de trabalho na nuvem e no local, agora você pode filtrar por todos os provedores de nuvem, todos os provedores no local ou provedores individuais.

  > **Observação:**
  >
  > O filtro é aplicado imediatamente após a seleção, sem um botão de aplicar.

- **Seleção de vários grupos de entrega**: Anteriormente, você só podia selecionar um único grupo de entrega (DG) ou todos os DGs. Agora, você pode selecionar até 15 DGs de uma vez. Se um site tiver menos de 15 DGs, você pode selecionar todos os DGs disponíveis. Você também pode excluir DGs específicos da seleção para visualizar dados para os DGs restantes.
- **Visão sobre máquinas com falha**: A página **Economia de custos** agora fornece visibilidade sobre máquinas em estado de falha ou não registradas. Os dois novos campos a seguir estão incluídos:
  - **Estado de falha sem sessões**: Este campo exibe a contagem de máquinas que estão em estado de falha e não têm sessões ativas.
  - **Não registrado com sessões**: Este campo exibe a contagem de máquinas que estão em um estado não registrado, mas ainda têm sessões ativas.

Você pode ver a contagem de máquinas nos estados precedentes e agir com base no motivo da falha, tempo e grupo de entrega. As contagens são links clicáveis que navegar para a página **Filtros** para ações adicionais. A contagem inclui máquinas de sessão única e de várias sessões.

> **Observação:**
>
> Os filtros são preservados na navegação entre páginas.

> Para obter mais informações, consulte a página Economia de custos.

Maio de 2025

Recursos novos e aprimorados

Compartilhe imagens preparadas criptografadas entre regiões no Azure. As imagens da Galeria de Computação do Azure (ACG) podem ser criptografadas com um Conjunto de Criptografia de Disco (DES). Com esse recurso, você pode compartilhar uma imagem ACG preparada criptografada entre várias regiões na mesma assinatura e locatário usando DES. Você pode, a partir daí, criar um catálogo de máquinas na região onde a imagem preparada criptografada é compartilhada. Para obter mais informações, consulte Compartilhar imagem preparada criptografada entre regiões.

Atualize as propriedades de VMs individuais no VMware. Agora você pode atualizar as propriedades de VMs individuais em um catálogo de máquinas MCS persistente usando um comando PowerShell. Essa implementação ajuda você a gerenciar VMs individuais de forma eficiente sem atualizar todo o catálogo de máquinas. Atualmente, esse recurso é aplicável apenas aos ambientes de virtualização Azure e VMware. Para obter mais informações, consulte Atualizar propriedades de VMs individuais.

Suporte para atualização de máquinas provisionadas por MCS em ambientes VMware. Em ambientes VMware, `Set-ProvScheme` altera o esquema de provisionamento e não afeta as máquinas existentes de um catálogo de máquinas MCS. Usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`, agora você pode aplicar o esquema de provisionamento atual a uma máquina ou conjunto de máquinas existente, persistente ou não persistente. Esse recurso é aplicável a catálogos de máquinas baseados em perfil de máquina e não baseados em perfil de máquina. Para obter mais informações, consulte Atualizar VMs provisionadas para o estado atual do esquema de provisionamento.

Estime os custos de VM do Azure durante a criação do catálogo. Ao criar um catálogo de máquinas, agora você pode estimar o custo mensal das máquinas virtuais do Azure, incluindo o tamanho da VM e os custos de disco. Você também pode refinar a estimativa ajustando configurações como horas diárias de funcionamento, dias úteis, planos de economia, instâncias

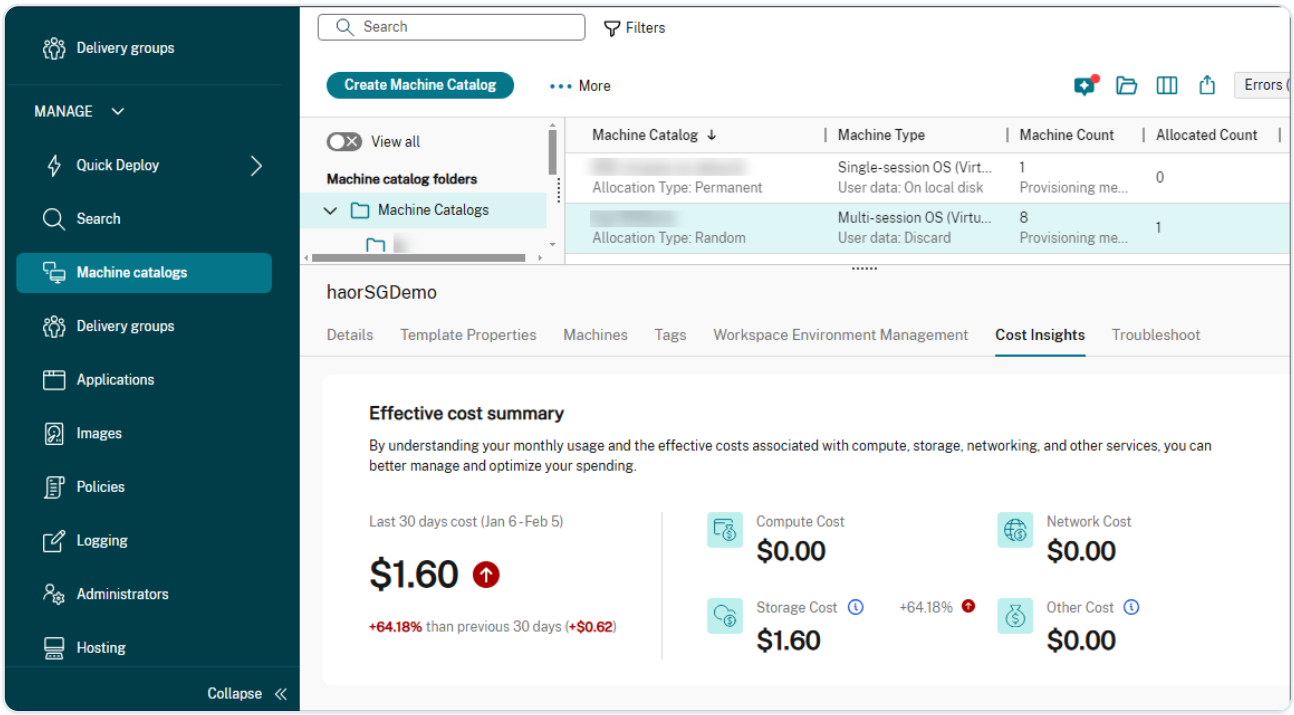
reservadas e armazenamento de desligamento. Esse recurso ajuda você a planejar implantações com mais eficiência e otimizar custos desde o início.

Para obter mais informações, consulte Exibir detalhes da estimativa mensal.

Visualização de insights de custos de provisionamento. Agora você pode visualizar informações detalhadas de custos para catálogos de máquinas. A visualização fornece uma visão geral dos custos de provisionamento e tendências dos últimos 30 dias.

O relatório detalha os custos de provisionamento com base em catálogos individuais, permitindo uma compreensão clara de como cada categoria contribui para o custo total. O relatório:

- Exibe o custo total incorrido nos últimos 30 dias.
- Compara o custo total atual de 30 dias com o período anterior de 30 dias.
- Exibe detalhes de custo de:
  - Custo de computação
  - Custo de armazenamento
  - Custo de rede
  - Outros custos



Para obter mais informações, consulte Exibir detalhes do catálogo.

Suporte para converter catálogos de máquinas de imagens mestre para imagens preparadas. Com uma nova ação, **Converter para Imagem Preparada**, no Studio, agora você

pode converter catálogos de máquinas provisionados por MCS que usam imagens mestre para catálogos que usam imagens preparadas. Os catálogos convertidos não podem ser revertidos. Este recurso está disponível para ambientes de virtualização Azure e VMware.

Para obter mais informações, consulte Converter catálogos provisionados por MCS de imagens mestre para imagens preparadas.

Configuração de proxy para contas de serviço. A criação de contas de serviço agora oferece suporte à configuração de proxy por meio do NGS Proxy para gerenciamento de identidade do Azure AD. Com este recurso, você pode:

- Excluir dispositivos Azure AD para catálogos unidos ao Azure AD
- Excluir dispositivos Intune para catálogos unidos ao Azure AD e registrados no Intune
- Criar, editar e excluir grupos de segurança do Azure AD

Para obter mais informações, consulte Criar uma conta de serviço do Azure AD.

Métricas de saúde do Connector Appliance. O componente **Connector Appliance** é adicionado por padrão como parte do monitoramento de infraestrutura. O componente **Connector Appliance** que está conectado ao site do Citrix DaaS é automaticamente integrado para monitoramento.

Este recurso permite que os clientes monitorem a saúde do Connector Appliance no painel de monitoramento de infraestrutura.

Você pode selecionar o tipo de **Componente** necessário e os detalhes são exibidos de acordo com o nome do site selecionado. Você também pode selecionar o **Local do recurso**. Para obter mais informações, consulte Métricas de saúde do Connector Appliance.

Abril de 2025

Recursos novos e aprimorados

Use o Autoscale para hibernar VMs. O gerenciamento de energia foi aprimorado para oferecer suporte à hibernação de VMs por meio de configurações configuráveis do Autoscale. Use os comandos do PowerShell `Get-BrokerDesktopGroups`, `New-BrokerDesktopGroups` ou `Set-BrokerDesktopGroups` para definir o seguinte valor positivo para o parâmetro `AutoscaleScaleDownActionDuringPeak` (durante o pico) ou `AutoscaleScaleDownActionDuringOffPeak` (fora do pico) para definir as ações de energia:

- 0: Desligar as VMs ao reduzir a escala
- 1: Suspender (hibernar as VMs) ao reduzir a escala

As VMs que não são capazes de hibernação são desligadas.

Autoscale Inteligente. O Autoscale Inteligente é um recurso de Autoscale baseado em dados com configurações administrativas mínimas que permite configurar o objetivo de desempenho de um grupo de entrega. O valor do objetivo de desempenho varia de 1 a 99 e o valor especifica um equilíbrio entre a experiência do usuário e o custo:

- Um valor baixo prioriza a economia de custos.
- Um valor alto prioriza a experiência do usuário.

O objetivo de desempenho, combinado com dados históricos de uso, calcula uma capacidade de buffer ideal (o número de VMs a serem ligadas) para cada bloco de 30 minutos de um dia. Portanto, 48 capacidades de buffer ideais são calculadas no início de cada dia.

A capacidade de buffer ideal substitui a capacidade de buffer de pico e fora de pico e o tamanho do pool para gerenciar as máquinas disponíveis.

Para obter mais informações, consulte plug-in de agendamentos do Autoscale Inteligente.

Studio: Suporte para exercer controle de acesso sobre aplicativos no nível do grupo de entrega. Anteriormente, no Studio, você só podia exercer controle de acesso sobre aplicativos no nível do aplicativo individual, não no nível do grupo de entrega. Agora, você pode realizar o controle de acesso sobre aplicativos no nível do grupo de entrega. Atualmente, essa capacidade é limitada ao controle de acesso a todos os aplicativos dentro de um grupo de entrega. Para obter mais informações, consulte Restringir o acesso a aplicativos a usuários específicos.

Filtro de Plataforma Cliente para atribuições de política. Agora você pode controlar as atribuições de política com mais precisão com um novo filtro, Plataforma Cliente. Este filtro permite atribuir (Permitir) ou excluir (Negar) políticas com base no sistema operacional dos dispositivos dos usuários, incluindo Windows, macOS, Linux, iOS, Android ou HTML5. Este aprimoramento oferece maior flexibilidade e precisão na atribuição de políticas, garantindo uma experiência personalizada e uniforme em dispositivos gerenciados e não gerenciados. Para obter mais informações, consulte Atribuições de política.

Opção para redefinir contas do Active Directory (AD) em uso. Com o Studio, agora você pode redefinir contas do Active Directory (AD) da máquina mesmo quando o status da máquina é Em Uso. Este aprimoramento é necessário porque, às vezes, o sistema não detecta corretamente quando uma máquina está em um estado *corrompido*.

Suporte para provisionamento de disco de dados no VMware. Um disco de dados permite o armazenamento de dados persistentes, como logs de eventos, rastreamentos de segurança e dados de aplicativos. Com este recurso, agora você pode criar e atribuir um disco de dados persistente e não persistente a uma VM persistente ou não persistente criada por MCS de um catálogo de máquinas MCS no VMware.

O disco de dados deve ser provisionado a partir da imagem mestre. O disco de dados da VM provisionada deriva propriedades como política de armazenamento, tamanho e assim por diante da imagem mestre. Para catálogos baseados em perfil de máquina, ele pode opcionalmente usar o disco de dados do modelo de VM para derivar as propriedades. Se o modelo de VM não tiver um disco de dados, a política padrão do Armazenamento será usada. Para obter informações sobre como criar um catálogo de máquinas MCS com um disco de dados, consulte Provisionar um disco de dados em uma VM criada por MCS.

Habilitar o Trusted Launch de catálogos persistentes e não persistentes existentes. Com este recurso, você pode atualizar um catálogo de máquinas persistentes e não persistentes existente sem Trusted Launch para um catálogo habilitado com Trusted Launch.

Para criar ou atualizar com sucesso um catálogo de máquinas com Trusted Launch, você deve usar um perfil de máquina. No entanto, se você usar uma imagem mestre habilitada com Trusted Launch e um perfil de máquina não habilitado com Trusted Launch, você receberá uma mensagem de aviso devido à configuração de Trusted Launch incompatível entre a imagem mestre e o perfil de máquina.

Para obter mais informações, consulte Catálogos de máquinas com Trusted Launch.

Gerenciamento simplificado de grupos de segurança do Azure AD usando contas de serviço. Anteriormente, o gerenciamento do grupo de segurança do Azure AD exigia que você fizesse login no Azure AD e obtivesse o token de acesso.

Com este aprimoramento, o MCS agora oferece suporte ao uso de uma conta de serviço pré-criada para gerenciar grupos de segurança do Azure AD para máquinas ingressadas no Azure AD. No entanto, para usar uma conta de serviço com capacidade de gerenciamento de grupo de segurança do Azure AD, você precisa de algumas permissões. Para obter informações, consulte Permissões necessárias para uma entidade de serviço do Azure AD.

Você pode usar a conta de serviço para fazer o seguinte sem a necessidade de obter o token de acesso.

- Criar um catálogo de máquinas com grupo de segurança dinâmico do Azure AD
- Habilitar o recurso de grupo de segurança para um catálogo do Azure AD

- Excluir um catálogo de máquinas com grupo de segurança de dispositivo ingressado no Azure AD
- Criar um grupo de segurança dinâmico do Azure AD sob um grupo de segurança atribuído do Azure AD existente

Para obter informações, consulte:

- Grupo de segurança dinâmico do Azure Active Directory
- Criar um grupo de segurança dinâmico do Azure AD sob um grupo de segurança atribuído do Azure AD existente

Suporte para a criação de catálogos ingressados no Azure AD Híbrido e catálogos ingressados no Azure AD Híbrido registrados no Microsoft Intune com imagens preparadas. Com este recurso, agora você pode usar imagens preparadas para criar catálogos ingressados no Azure AD Híbrido e catálogos ingressados no Azure AD Híbrido registrados no Microsoft Intune usando comandos do Studio e do PowerShell. Este recurso é aplicável a catálogos MCS de tipo persistente e não persistente de sessão única e multi-sessão. No entanto, atualmente, você pode criar catálogos para catálogos ingressados no Azure AD Híbrido registrados no Microsoft Intune apenas para VMs persistentes de sessão única e multi-sessão. O registro de VMs não persistentes ingressadas no Azure AD Híbrido no Microsoft Intune está atualmente em visualização.

Esta implementação reduz significativamente os custos de armazenamento e tempo, e simplifica o processo de implantação de VM e atualização de imagem. Para o conjunto completo de comandos do PowerShell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada, consulte Usar PowerShell. Para obter informações sobre como criar um catálogo ingressado no Azure AD Híbrido e catálogos ingressados no Azure AD Híbrido registrados no Microsoft Intune, consulte Pool de identidades de identidade de máquina ingressada no Azure Active Directory Híbrido e Criar catálogos ingressados no Azure AD Híbrido registrados no Microsoft Intune.

Suporte para SCVMM 2025. O Citrix DaaS agora oferece suporte ao System Center Virtual Machine Manager (SCVMM) 2025 da Microsoft. O SCVMM fornece uma variedade de serviços para incluir a manutenção dos recursos necessários para implantar VMs. Para obter mais informações sobre os novos recursos suportados no SCVMM 2025, consulte Novidades no System Center Virtual Machine Manager.

Suporte para o uso automático do Disco Temporário do Azure para o disco de cache de write-back. Ao editar um catálogo provisionado por MCS no Studio, o catálogo agora usa automaticamente o Disco Temporário do Azure para o disco de cache de write-back (WBC) se os

critérios necessários forem atendidos. Como resultado, as novas VMs adicionadas ao catálogo usam o Disco Temporário do Azure para o disco WBC.

Anteriormente, se um catálogo não se qualificasse na criação, o Disco Temporário do Azure não era usado para o disco WBC — mesmo que o catálogo fosse atualizado posteriormente para atender aos critérios.

Benefícios:

- Reduza os custos. Os Discos Temporários não incorrem em custos de armazenamento quando a VM é desligada.
- Melhore a flexibilidade. Use Discos Temporários para WBC sem recriar o catálogo.

Um catálogo provisionado por MCS usa automaticamente o Disco Temporário do Azure para o disco WBC quando o catálogo atende a todos os seguintes critérios:

- MCSIO está ativado.
- O disco WBC não é persistente.
- O tamanho da VM inclui um Disco Temporário grande o suficiente para o disco WBC.
- Nenhuma letra de unidade é especificada para o disco WBC.

Para obter mais informações, consulte Criar um catálogo do Microsoft Azure.

Suporte para controle de visibilidade de aplicativos para usuários do Azure AD. Anteriormente disponível apenas para usuários do Active Directory, a capacidade de restringir a visibilidade de aplicativos agora é estendida aos usuários do Azure AD. Com o Studio, agora você pode controlar quais usuários e grupos do Azure AD podem ver um aplicativo específico no aplicativo Workspace.

Esta função requer a versão 2411 do VDA ou posterior. Para obter mais informações sobre as etapas detalhadas, consulte Alterar propriedades do aplicativo > Limitar visibilidade.

Março de 2025

Recursos novos e aprimorados

Opção de reconfiança para certificados de conexão de host não confiáveis. Se ocorrer uma interrupção na conexão do host devido a um certificado não confiável, você poderá reconfiar no certificado para essa conexão de host no Studio. Para obter mais informações, consulte Testar a confiança do certificado TLS.

Ressincronizar implantações na interface do usuário do AWS. Uma nova opção para ressincronizar implantações no AWS foi adicionada. Ressincronize uma implantação que esteja no estado Pendente ou se o número de máquinas listadas em uma implantação não corresponder ao número de máquinas listadas no AWS.

> **Nota:**
>
> - Quando uma implantação no estado Ativo ou Erro está ressincronizando, o status dessa implantação muda para **Sincronizando máquinas**.
> - Quando uma implantação no estado Pendente está ressincronizando, o status continua a ser exibido como **Pendente** até ser concluído.

> Para obter mais informações, consulte Criar uma implantação.

O gerenciamento centralizado de sites está geralmente disponível. Como Administrador de Nuvem de vários sites, agora você pode designar um site como principal e vincular outros sites a ele para um gerenciamento centralizado e simplificado. Esse recurso ajuda a melhorar a eficiência operacional, reduzindo a necessidade de alternar entre sites para tarefas diárias.

Principais benefícios:

- **Gerenciamento eficiente de sites**: Os administradores podem gerenciar vários sites a partir de uma única interface, alternando entre eles usando o menu suspenso no canto superior direito, eliminando a necessidade de trocar de conta.
- **Navegação contínua**: Os administradores podem alternar facilmente entre o Studio e o Monitor sem precisar selecionar novamente o site. Quando um site é selecionado no Studio, ele é automaticamente selecionado no Monitor, otimizando seu fluxo de trabalho.
- **Operações de help desk simplificadas**: Os administradores de help desk podem visualizar informações de todos os sites em um único console do Monitor.
- **Experiência agregada do usuário final**: Os usuários finais fazem login em uma única URL do Citrix Workspace (por exemplo, customer.cloud.com) para acessar recursos de sites vinculados.

Para obter mais informações, consulte Gerenciamento centralizado de sites.

Aprimoramentos da interface do usuário no Studio. O Web Studio apresenta as seguintes melhorias para aprimorar a eficiência da sua administração:

- Copiando dados de tabelas

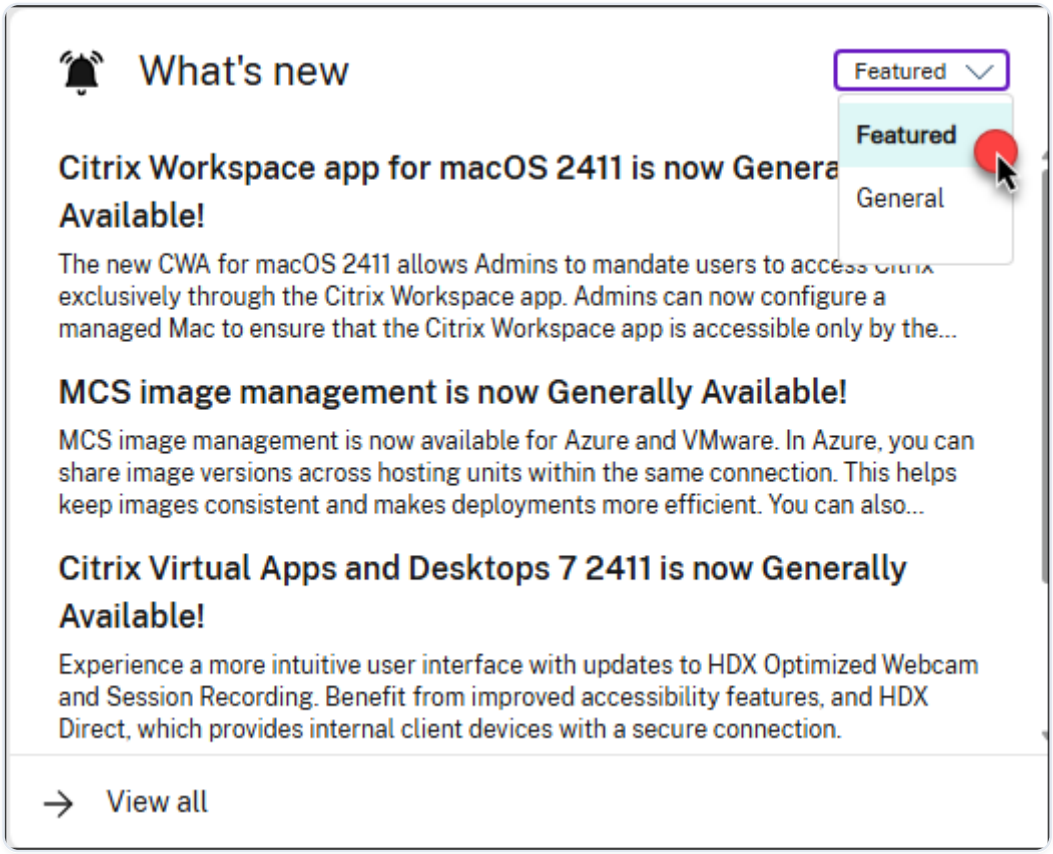
  Agora você pode copiar dados diretamente de componentes de tabela, como "Nome da máquina" na tabela Alocação de Máquinas. Este aprimoramento reduz a necessidade de entrada manual de dados, minimizando o risco de erros.

- Paginação para tabelas

  Os componentes de tabela agora suportam paginação, aumentando o desempenho e a usabilidade.

Aprimoramento do widget Novidades. Um novo recurso foi introduzido no widget Novidades na página **Início** do Studio. Agora você pode alternar facilmente entre duas fontes de conteúdo:

- **Destaques**: Conteúdo selecionado e escolhido a dedo para insights e destaques rápidos do produto.
- **Geral**: Uma lista abrangente de conteúdo obtido diretamente da documentação do DaaS para atualizações de recursos aprofundadas e extensas. Esta atualização garante que você tenha a flexibilidade de acessar conteúdo selecionado e extenso, aprimorando sua experiência e mantendo você bem informado.



Limite de uso de token na inscrição baseada em token aumentado para 5000. Aumentamos o limite de uso de token na inscrição baseada em token de 100 para 5000, permitindo maior flexibilidade ao inscrever máquinas em catálogos de máquinas de grande capacidade.

Para obter mais informações, consulte Gerar e gerenciar tokens de inscrição.

Migração de VMs não persistentes no VMware. Anteriormente, no ambiente VMware, você podia migrar apenas os discos de VM persistentes de um armazenamento para outro. Com este recurso, você pode migrar os discos de VM não persistentes de um armazenamento para outro usando o comando PowerShell `Move-ProvVMDisk`. Você pode migrar: Disco do SO, Disco de Identidade e disco de Cache de Gravação (WBC).

Para obter mais informações, consulte Migração de armazenamento de VMs.

Migração de VMs persistentes e não persistentes no XenServer®. Com este recurso, no ambiente XenServer, você pode migrar os seguintes discos de VM de um armazenamento para outro usando o comando PowerShell `Move-ProvVMDisk`.

- Para VMs de clone completo persistentes: Disco do SO, Disco de Identidade e discos provisionados não-MCS.
- Para VMs não persistentes: Disco do SO, Disco de Identidade e disco de Cache de Gravação (WBC).

Para obter mais informações, consulte Migração de armazenamento de VMs.

Recursos aprimorados do Autoscale para melhor gerenciamento de energia. Aprimoramos o Autoscale para melhorar suas experiências. Agora você pode:

- Receber notificações se as máquinas em um grupo de entrega não suportarem hibernação, juntamente com recomendações para ações alternativas, como desligar essas máquinas.
- Escolher suspender máquinas em vez de pará-las, onde for suportado.
- Definir agendamentos de reinício para máquinas suspensas para evitar que permaneçam suspensas indefinidamente.

Para obter mais informações, consulte Configurações baseadas em agendamento e Configurações baseadas em carga.

Melhoria no dimensionamento de carga de trabalho. A guia **Dimensionamento de carga de trabalho** (anteriormente Dimensionamento de Infraestrutura) agora inclui uma opção para identificar usuários avançados. Este recurso permite exportar os detalhes dos usuários avançados.

> **Nota:**

> Este recurso está disponível apenas para grupos de entrega de SO de sessão única.

> Os dados de **Exportação** incluem **Nome de Usuário**, **Contagem Total de Sessões**, **Duração Média da Sessão (Minutos)**, **Uso Máximo da CPU (%)** e **Uso Máximo da Memória (%)**.

Este aprimoramento fornece informações valiosas sobre a utilização de recursos e ajuda a otimizar os custos de infraestrutura, garantindo uma alocação eficiente de recursos com base no comportamento do usuário. Para obter mais informações, consulte a página Dimensionamento de carga de trabalho.

Aprimoramento na guia Desempenho da Sessão. A seção **Topologia da Sessão** da guia **Desempenho da Sessão** foi aprimorada para incluir o seguinte:

- **Protocolo**: Exibe o valor MTU para o protocolo EDT. Por exemplo:
  - Fluxo único: EDT (MTU = 1500)
  - Multifluxo: EDT (IDs de fluxo MTU 0=1500, 1=1500)
- **MS Teams**: Exibe se otimizado para HDX ou não otimizado para HDX.
- **Tipo de Conexão HDX**: Exibe o tipo de conexão HDX. Por exemplo: HDX, HDX Direct e Rendezvous.
- **Quadros por Segundo** fornece informações sobre:
  - Quadros de Entrada por Segundo
  - Quadros de Saída por Segundo

As configurações de grupos de segurança são herdadas de perfis de máquina. Agora você pode criar um catálogo de máquinas MCS e selecionar um perfil de máquina que tenha grupos de segurança atribuídos. Isso evita a configuração do grupo de segurança, pois ela é herdada do perfil da máquina. Alternativamente, se você não selecionar um perfil de máquina, no momento da criação do catálogo de máquinas MCS, configure os grupos de segurança na página Segurança no Studio. Para obter mais informações, consulte Segurança.

Plug-in de feriado do Autoscale. Com este recurso, você pode desviar das configurações padrão do Autoscale relacionadas ao gerenciamento de energia de VMs e permitir que as VMs sejam desligadas em datas de feriado especificadas. Por exemplo, para dias úteis, você deseja que a maioria das VMs esteja ligada e, por padrão, em feriados públicos, o agendamento de dias

úteis é aplicado. Para gerenciar tais cenários, use o plug-in de feriado do Autoscale para desligar as VMs em datas de feriado especificadas.

Para obter mais informações, consulte Plug-in de feriado do Autoscale.

Corresponder o programa de inicialização UEFI à versão do Citrix Provisioning para catálogos do Citrix Provisioning criados pelo MCS. O servidor Citrix Provisioning usa um disco BDM, que contém um programa de inicialização UEFI. Este recurso permite a geração do arquivo `BOOTX64.EFI` junto com o arquivo `PVSBOOT.INI` ao criar um catálogo do Citrix Provisioning usando o MCS. Como resultado, os dispositivos de destino podem inicializar a partir do arquivo de configurações de inicialização mais recente, garantindo que os dispositivos de destino estejam alinhados com a versão do Citrix Provisioning.

Suporte para a criação de catálogos ingressados no Azure AD e registrados no Microsoft Intune com imagens preparadas. Com este recurso, agora você pode usar imagens preparadas para criar catálogos ingressados no Azure Active Directory e registrados no Microsoft Intune usando comandos do Studio e do PowerShell. Este recurso é aplicável a catálogos MCS de tipo persistente e não persistente de sessão única e multi-sessão. Esta implementação reduz significativamente os custos de armazenamento e tempo, e simplifica o processo de implantação de VM e atualização de imagem. Para o conjunto completo de comandos Powershell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada, consulte Usar PowerShell. Para obter informações sobre como criar um catálogo ingressado no Azure AD e um catálogo do Azure AD registrado no Microsoft Intune, consulte Pool de identidade de máquina ingressada no Azure Active Directory e Criar catálogos do Azure AD registrados no Microsoft Intune.

Opção de localização de armazenamento flexível para VMs. Anteriormente, a alocação de VM começava de um Serviço de Armazenamento (SR) fixo, como SR1, e progredia sequencialmente através de SR2, SR3 e assim por diante. E, em alguns casos, a carga de armazenamento não é distribuída uniformemente entre os armazenamentos.

Este recurso oferece a capacidade de equilibrar a alocação de VM entre diferentes serviços de armazenamento usando os seguintes métodos:

- **Método de alocação round robin atual aprimorado**: Em vez de sempre começar do mesmo SR fixo, o MCS agora inicia a alocação do SR logo após o último SR usado.
- **Método de alocação baseado na menor carga**: Coloca as VMs na menor carga atual, determinada comparando o número total de VMs em cada SR dentro do mesmo catálogo de máquinas. Por exemplo, se um catálogo de máquinas contém 100 VMs distribuídas da seguinte forma: 20 VMs em SR1, 30 VMs em SR2 e 50 VMs em SR3, as novas VMs são

alocadas primeiro para SR1. Este método garante que a carga entre SR1, SR2 e SR3 seja equilibrada. Você pode usar este método adicionando uma propriedade personalizada Nome=`"StorageBalanceType"` Valor=`"VMCountBasedLeastLoad` ao criar ou atualizar uma conexão de host.

Este recurso é:

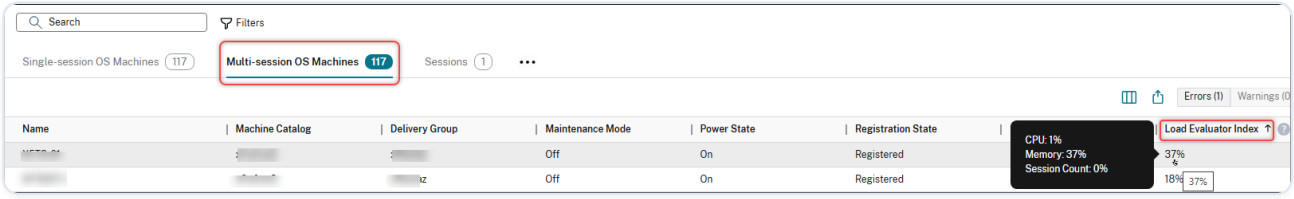
- Aplicável a todos os hipervisores locais (VMware, XenServer e Hyper-V).
- Aplicável apenas ao armazenamento em disco do SO.
- Não aplicável às VMs existentes.

Para obter informações sobre como criar ou atualizar uma conexão de host existente com a opção de alocação baseada em carga, consulte Opção de local de armazenamento flexível para VMs.

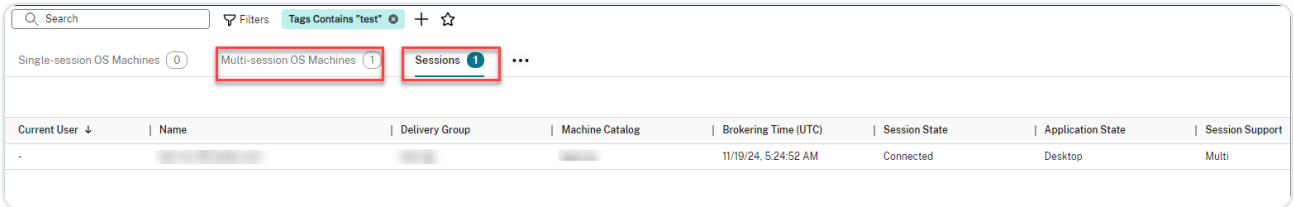
Monitoramento de recursos aprimorado para VDAs multissessão no Studio. O Studio agora fornece insights detalhados sobre a utilização de recursos e capacidades para VDAs multissessão.

Passe o mouse sobre a coluna **Load Evaluator Index** de um VDA multissessão no nó **Pesquisar** para visualizar métricas detalhadas, incluindo CPU, memória, uso de disco, número máximo de sessões permitidas e muito mais. As métricas específicas exibidas dependem das configurações de política ativadas.

Este aprimoramento elimina a necessidade de executar cmdlets do PowerShell ou navegar por várias etapas para alternar para o Monitor para coletar esses dados, fornecendo as mesmas capacidades diretamente no Studio. Para obter mais informações, consulte Ações da máquina.



Visibilidade aprimorada da sessão em pesquisas baseadas em tags. Ao pesquisar *máquinas* por tag em **Studio > Pesquisar**, as *sessões* de usuário ativas nas máquinas correspondentes agora aparecem na guia **Sessões**. Este aprimoramento ajuda a evitar desligamentos acidentais de máquinas com sessões ativas, fornecendo visibilidade clara dessas sessões, melhorando sua eficiência de gerenciamento.



Fevereiro de 2025

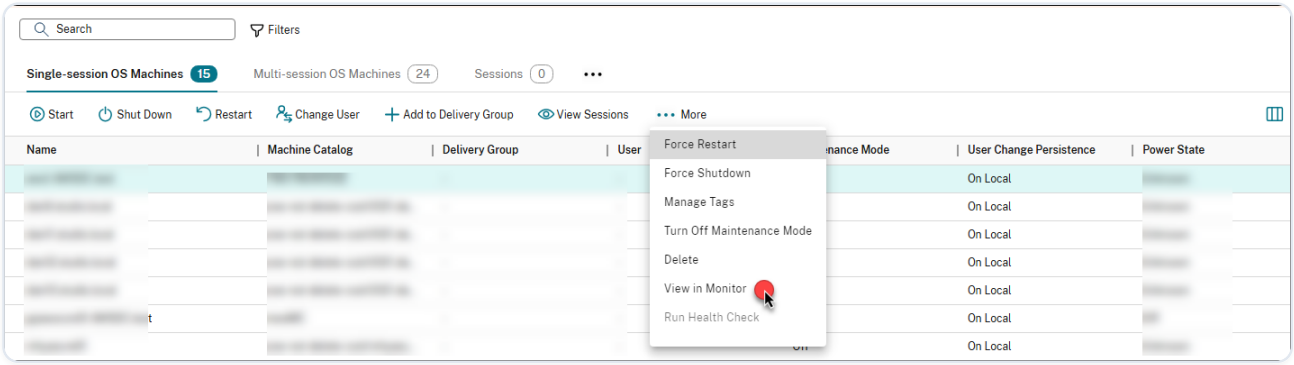
Recursos novos e aprimorados

Suporte para provisionamento de disco de dados no Azure. Agora você pode criar e atribuir um disco de dados persistente a uma VM persistente ou não persistente criada por MCS de um catálogo de máquinas MCS no Azure. O disco de dados é usado para armazenamento de dados persistentes, como logs de eventos, rastreamentos de segurança e dados de aplicativos.

O disco de dados deve ser provisionado a partir da imagem mestre. As propriedades, como tipo de armazenamento, configurações de criptografia e zonas, são derivadas de propriedades personalizadas ou do modelo de disco do SO, se as propriedades não forem especificadas nas propriedades personalizadas. Para obter informações sobre como criar um catálogo de máquinas MCS com um disco de dados, consulte Provisionar disco de dados.

navegar sem problemas do Studio para o Monitor para máquinas e sessões. Uma nova opção, **Exibir no Monitor**, agora está disponível em **Studio > Pesquisar**, fornecendo acesso mais rápido a informações detalhadas de sessão e máquina no **Monitor**.

Após selecionar uma máquina ou sessão, basta clicar em **Exibir no Monitor** para abrir sua visualização detalhada no **Monitor**. Este aprimoramento simplifica seu fluxo de trabalho e economiza tempo ao analisar o desempenho da carga de trabalho ou solucionar problemas. Para obter mais informações, consulte Ações da máquina e Ações da sessão.



Economia de custos otimizando o uso do armazenamento. A página **Economia de Custos** agora oferece visibilidade sobre o valor da economia alcançada por meio da otimização do armazenamento quando as máquinas são desligadas. Anteriormente, apenas a economia de custos relacionada à computação era exibida. Este aprimoramento inclui os dois tipos de economia de armazenamento a seguir:

- **Disco de gravação (Write-back Disk)**: Economia resultante da exclusão do disco de gravação quando uma máquina não persistente é desligada.

- **Disco do SO**: Economia resultante do downgrade do disco do SO de Premium para HDD Padrão quando qualquer máquina é desligada.

Pré-requisito:

- O Autoscale deve estar habilitado para otimizar os custos de computação. Para obter mais informações, consulte Introdução ao Autoscale.
- Altere o tipo de armazenamento para um nível inferior quando uma VM for desligada para otimizar os custos de armazenamento. Para obter mais informações, consulte a documentação Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada.
- Este recurso é atualmente aplicável apenas a máquinas Azure.

O aprimoramento inclui:

- Um relatório detalhando a economia de armazenamento de desligamentos de máquinas (autoscale ou iniciados pelo usuário) agora está disponível na seção **Economia de infraestrutura estimada**.
- Os cálculos de economia total agora incorporam tanto a economia de computação quanto a de armazenamento, discriminadas por origem (autoscale ou ação do usuário). O gráfico de tendência histórica agora distingue visualmente entre a economia de computação e de armazenamento, e uma dica de ferramenta fornece mais detalhes ao passar o mouse.
- A seção **Detalhes do catálogo** agora inclui **Custo de computação por hora** e **Custo de armazenamento por hora**.

Para obter mais informações, consulte a página Resumo de custos.

Capacidade de inicialização segura NitroTPM e UEFI para instâncias de VM AWS criadas por MCS. Com este recurso, ao criar um catálogo em ambientes AWS, agora você pode selecionar uma imagem mestre (AMI) com NitroTPM e/ou inicialização segura UEFI habilitados. Consequentemente, as VMs provisionadas no catálogo também são habilitadas com NitroTPM e/ou inicialização segura UEFI. Esta implementação garante que as VMs sejam seguras e confiáveis. Para obter mais informações sobre NitroTPM e inicialização segura UEFI, consulte a documentação da AWS. Para criar um catálogo habilitado com NitroTPM e inicialização segura UEFI, consulte Habilitar NitroTPM e inicialização segura UEFI para instâncias de VM.

Aprimoramentos de ação do Monitor O Citrix Monitor agora fornece o progresso das ações em massa realizadas, juntamente com melhorias nos acessos baseados em função em ações em massa, aprimorando a experiência e o controle do usuário.

Barra de Progresso da Ação:

Com este aprimoramento, quando qualquer ação estiver em andamento, como uma função de controle de energia (por exemplo, reinicialização), você poderá ver o status da ação e uma caixa de diálogo quando a ação for concluída. Este recurso é aplicável a todas as ações na guia **Filtros**. No entanto, observe que a barra de status não estará disponível para ações únicas.

A barra de progresso mostra os resultados das ações em massa realizadas. Atualmente, os clientes não sabem se a ação foi bem-sucedida ou falhou e em quantas sessões. Este aprimoramento fornece clareza sobre as ações realizadas.

Função personalizada para limitar a opção de ação em massa para ações do usuário:

Este aprimoramento permite a adição de funções personalizadas para limitar o que o administrador pode ver e controlar. A nova função personalizada limita a capacidade de selecionar ações em massa, como logoff, desconexão ou mensagem. Esse controle é necessário para evitar ações em massa não intencionais ou maliciosas em usuários.

Com esses aprimoramentos, você pode gerenciar e controlar efetivamente as ações no Citrix Monitor, garantindo um ambiente mais seguro e eficiente. Para obter mais informações, consulte Função personalizada para limitar a opção de ação em massa para ações do usuário.

Opção para visualizar e solucionar problemas de sessões de Acesso Privado Seguro para implantações híbridas. O Citrix Monitor agora oferece suporte à visualização e solução de problemas de sessões de Acesso Privado Seguro para implantações híbridas. Este aprimoramento permite que os clientes DaaS que usam Gateway, StoreFront e Acesso Privado Seguro no local monitorem e solucionem problemas de seus dados de sessão diretamente no DaaS Monitor.

Anteriormente, apenas implantações em nuvem e no local eram visíveis no Monitor. Com esta atualização, as sessões híbridas de Acesso Privado Seguro agora podem ser monitoradas e analisadas, fornecendo uma visão unificada em todos os tipos de implantação.

Esta melhoria garante melhor visibilidade, resolução mais rápida de problemas e uma experiência de monitoramento contínua para clientes que gerenciam ambientes híbridos. Para obter mais informações, consulte Integração do Acesso Privado Seguro com o Monitor (Pré-visualização).

Compartilhe versões de imagens preparadas entre unidades de hospedagem no VMware. Agora você pode usar o **nó Imagens** para compartilhar versões de imagens entre unidades de hospedagem dentro da mesma conexão de hospedagem no VMware. Esta implementação garante a consistência e uniformidade das imagens em diferentes unidades de host, aprimorando a flexibilidade de implantação e a eficiência operacional. Você também pode usar comandos

PowerShell para atingir esse objetivo. Para obter mais informações, consulte Gerenciamento de Imagens

Janeiro de 2025

Recursos novos e aprimorados

Suporte para a criação de catálogos de máquinas MCS habilitados para MCSIO na AWS. Agora você pode criar catálogos MCS habilitados para MCSIO para criar catálogos de máquinas MCS habilitados para MCSIO na AWS para melhorar as IOPS de gravação, direcionando as operações de gravação para o cache de write-back e para reduzir o tempo de inicialização quando o disco do SO persistente está habilitado. Para obter mais informações, consulte Otimização de armazenamento do Machine Creation Services (MCS).

Integração com Webhook O Citrix Monitor agora se integra ao Webhook. Usando este recurso, você pode selecionar a ferramenta necessária na seção **Alertas e ITSM** na página **Integrações e exportações de dados** e, em seguida, clicar em **Começar**. Isso fornece links de referência para criar o canal específico da ferramenta e o URL do webhook, que é o primeiro passo. Uma vez concluído o primeiro passo, você pode criar perfis de webhook.

Você também pode criar perfis de webhook na página **Integrações e exportações de dados** > **Ferramentas do desenvolvedor** do Citrix Monitor. Você pode encontrar etapas e recursos para integrar as seguintes ferramentas de alerta e ITSM com o Citrix Monitor:

- Slack
- Microsoft Teams
- ServiceNow

Este recurso ajuda você a enviar notificações de alerta para os aplicativos de terceiros anteriores que têm URLs de webhook de entrada configuradas.

Principais recursos:

- Novos blocos de integração para Slack, Teams, ServiceNow e outras plataformas suportadas
- Navegação para a página FTU para cada integração
- Página de criação ou edição de configuração de webhook com um fluxo de trabalho de UI para fornecer URL de webhook, cabeçalhos, corpo e testar a configuração do webhook e salvá-la
- Listar os perfis de webhook criados e fornecer a capacidade de editar ou excluir os perfis de webhook

- Mapear perfis de webhook criados com as políticas de alerta avançadas

Para obter mais informações, consulte a página Integrações e exportações de dados.

Adicionar aplicativos a implantações AWS existentes no nó de implantação rápida. Agora você pode adicionar aplicativos a implantações AWS existentes, simplificando assim o processo geral de implantação. Para obter mais informações, consulte Criar uma implantação.

Opção para redefinir contas do Active Directory (AD) em uso. Com o Studio, agora você pode redefinir contas do Active Directory (AD) da máquina mesmo quando o status da máquina é Em Uso. Isso é necessário porque, às vezes, o sistema não detecta corretamente quando uma máquina está em um estado corrompido.

Alertando os administradores de que as políticas de energia permanecem eficazes ao desabilitar o Autoscale. O aprimoramento visa lembrar os administradores de que a desativação do Autoscale não afeta as configurações da política de energia para um grupo de entrega. Isso garante que os administradores estejam cientes do escopo da desativação do Autoscale e esclarece que as políticas de energia permanecem eficazes quando o Autoscale é desativado.

Filtrar imagens mestre com base nas regiões da unidade de hospedagem. Durante a criação de catálogos de máquinas para a plataforma Azure, o Studio agora pode filtrar e excluir imagens mestre que pertencem a regiões diferentes da região da unidade de hospedagem. Isso garante que apenas imagens da mesma região da unidade de hospedagem estejam disponíveis para seleção. Para obter mais informações, consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas.

MCSIO com apenas cache de disco não é mais suportado. A opção de configurar o MCSIO com apenas cache de disco (sem cache de memória) foi removida em todos os ambientes de hipervisor e serviço de nuvem. Ao criar catálogos de máquinas com o MCSIO habilitado, agora você deve definir um tamanho de cache de memória diferente de zero. Além disso, você não pode editar catálogos configurados com apenas um cache de disco até definir um tamanho de cache de memória. Para obter mais informações, consulte Configurar cache para dados temporários.

A criação de VMs AWS usando propriedades de modelo de máquina não é mais suportada. O suporte para a criação de VMs AWS capturando propriedades de modelo de máquina foi removido como parte da transição para a criação de VMs usando perfis de máquina. A opção **Aplicar propriedades de modelo de máquina a máquinas virtuais** foi removida da página **Modelo de Máquina**. Em vez disso, você pode criar VMs AWS usando perfis de máquina para uma experiência semelhante e mais simplificada. Para obter mais informações, consulte Criar um

catálogo de máquinas baseado em perfil de máquina usando o Studio e Criar um catálogo de máquinas baseado em perfil de máquina usando o PowerShell.

Suporte para a criação de catálogo de máquinas MCS habilitado para MCSIO na AWS. No ambiente AWS, agora você pode criar um catálogo não persistente habilitado para Otimização de Armazenamento MCS (MCSIO) usando comandos PowerShell. Para criar tal catálogo, você deve instalar o driver MCSIO durante a instalação ou atualização do VDA. Por padrão, esse driver não é instalado. Para obter mais informações sobre a criação do catálogo habilitado para MCSIO, consulte Catálogo habilitado para MCSIO. A opção de configurar o MCSIO com apenas cache de disco (sem cache de memória) usando o Studio foi removida em todos os hipervisores e ambientes de serviço de nuvem.

Relatório de aplicativos publicados menos usados e não utilizados. A página **Aplicativos** agora oferece informações detalhadas de uso para aplicativos publicados acessados através do aplicativo Citrix Workspace, capacitando os administradores a otimizar o gerenciamento de aplicativos e a alocação de recursos.

Este recurso ajuda a entender os padrões de uso de aplicativos dentro da organização e permite que os clientes tomem decisões baseadas em dados para tornar suas implantações Citrix mais eficientes.

> **Nota:**

> Este recurso está disponível apenas para sites com licença platinum.

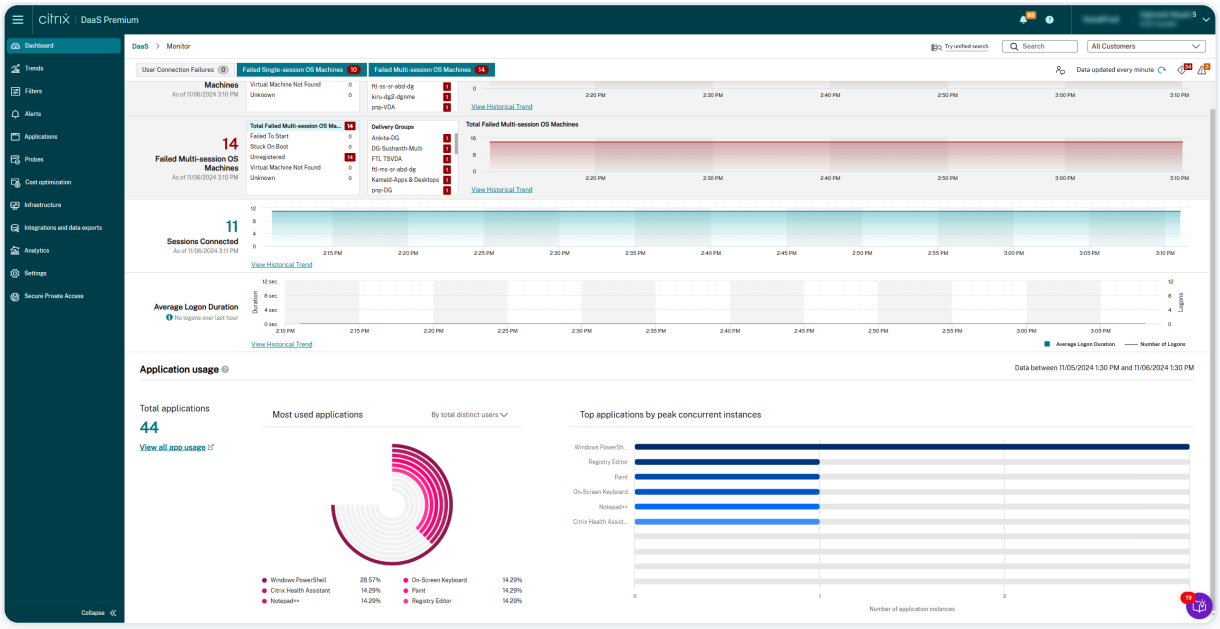
> A página **Aplicativos** aprimorada inclui uma seção de uso que mostra o seguinte:

- **Total de aplicativos publicados:** Identifica o número total de aplicativos publicados.
- **Aplicativos menos usados:** Ajuda a tomar decisões informadas sobre a retenção ou remoção de aplicativos raramente usados, otimizando a alocação de recursos e o gerenciamento de licenças. Esta seção lista o seguinte:
  - **Usuários distintos nos últimos 30 dias**
  - **Total de inicializações**
  - **Pico de instâncias simultâneas**
  - **Gráfico de tendências:** Visualize um gráfico mostrando usuários distintos ao longo do tempo.

- **Aplicativos não utilizados:** Ajuda a identificar aplicativos não utilizados para liberar memória, recursos de configuração e, potencialmente, economizar nos custos de licenciamento. Esta seção lista o nome dos aplicativos, o grupo de entrega correspondente e o estado do aplicativo.

Você também pode usar a opção **Exportar** para exportar os dados nas seções **Menos usados** e **Não utilizados**.

> **Nota:**
>
> Atualmente, apenas aplicativos publicados (aplicativos de desktop no aplicativo Citrix Workspace) estão incluídos nesta melhoria.



Para obter mais informações, consulte a documentação Relatório de aplicativos publicados menos usados e não utilizados.

Integração do Secure Private Access com o Monitor (Pré-visualização). A integração do Secure Private Access com o Monitor permite que o administrador monitore e solucione problemas de todas as sessões do Secure Private Access no Monitor.

As ações disponíveis incluem a visualização dos detalhes do seguinte:

- Sessões ativas do Secure Private Access para um usuário em Selecionar uma sessão pop-up > guia Sessões Ativas
- Enumerações falhas ou bloqueadas do Secure Private Access e inicializações de aplicativos falhas em Selecionar uma sessão pop-up > guia Acesso Negado

- Visualização de detalhes da sessão e do aplicativo para inicializações de aplicativos ativas e falhas, bem como para enumerações falhas e bloqueadas

Para obter mais informações, consulte a página de integração do Secure Private Access com o Monitor (Pré-visualização).

Dezembro de 2024

Recursos novos e aprimorados

Comandos da ferramenta de configuração automatizada para backup e restauração. Com este recurso, você pode usar comandos PowerShell suportados pela ferramenta de configuração automatizada para acionar as APIs de backup e restauração que o Studio usa. Para obter mais informações, consulte Cmdlets da ferramenta de configuração automatizada para backup e restauração.

Nova permissão para detecção de recursos órfãos no Citrix DaaS. Anteriormente, apenas as funções de **Administrador Completo** ou **Administrador de Nuvem** podiam realizar a detecção de recursos órfãos. Com a introdução da permissão **Usar Conexão de Host para Detectar Recursos Órfãos no Hypervisor** na categoria **Hosts**, qualquer função atribuída a esta permissão agora pode detectar recursos órfãos. Para obter mais informações, consulte Detectar recursos órfãos do Azure e Recuperar uma lista de recursos órfãos.

Comece a usar o Citrix DaaS no Google Cloud. A integração do Google Cloud Platform (GCP) com o Citrix DaaS e a implantação do primeiro conjunto de desktops virtuais envolve uma série de etapas sequenciais, tornando-o um processo relativamente intrincado. Para simplificar esse processo para os administradores, foi introduzida uma experiência de implantação simplificada, semelhante ao recurso Quick Deploy do AWS WorkSpaces Core. Este processo de integração simplificado visa aumentar a adoção do GCP, levando as equipes de vendas do Google a colaborar com a Citrix em engajamentos com clientes. Além disso, abre caminhos para as equipes de vendas da Citrix se engajarem com clientes que priorizam soluções centradas no Google. Para obter mais informações, consulte Implantação Rápida para Google Cloud.

Configuração Completa: Suporte para seleção de modelo de inicialização como perfil de máquina para AWS. Ao provisionar VMs AWS usando MCS, agora você pode selecionar um modelo de inicialização como perfil de máquina. Para obter mais informações, consulte Selecionar uma imagem e um perfil de máquina.

Políticas de seleção múltipla. Agora você pode selecionar várias políticas e verificar as seguintes melhorias:

- Clique em uma linha de política: Se você clicar em uma linha de política, a barra de ações na parte superior mostra as ações de uma única política. O painel de detalhes na parte inferior fornece informações sobre a política.
- Selecione as caixas de seleção de várias políticas: Se você selecionar as caixas de seleção de várias políticas cujos status estão habilitados ou desabilitados, a barra de ações na parte superior mostra as ações de várias políticas. O painel de detalhes na parte inferior exibe o número de políticas selecionadas.

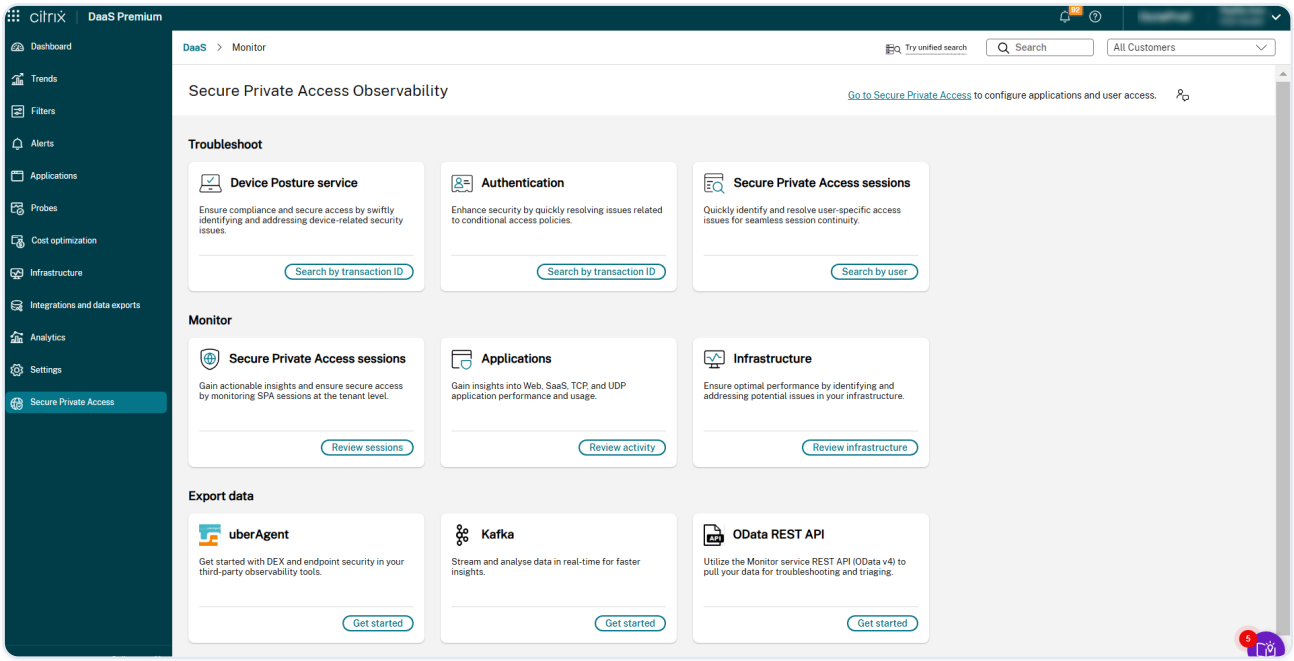
Nota:

Depois de selecionar várias políticas, você pode visualizar os detalhes de outra política individual clicando na linha dessa política. Esta ação não limpa as políticas selecionadas anteriormente. No entanto, a ação de clique com o botão direito não exibe as ações para aquela linha de política.

Catálogos GCP suportam a herança das configurações de tipo de máquina de perfis de máquina. Ao criar catálogos de máquinas provisionados por MCS em ambientes GCP, o tipo de máquina agora assume o tamanho especificado no perfil de máquina selecionado por padrão. Se necessário, você pode ajustar manualmente essa configuração. Para obter mais informações, consulte Criar um catálogo de máquinas usando a interface de Configuração Completa.

Clareza sobre políticas dependentes. Algumas configurações dependem de outras configurações. Por exemplo, uma configuração filha pode ser configurada, mas se sua configuração pai não estiver habilitada, a configuração filha configurada não terá efeito. As dependências não eram claras antes. A partir desta versão, é fornecida clareza sobre quais são as políticas pai que devem ser configuradas primeiro antes que você possa configurar as políticas filhas. Para obter mais informações, consulte Configurações de política.

Guia Secure Private Access no Monitor. A guia **Secure Private Access** no Monitor oferece um local dedicado para todos os novos recursos relacionados ao Secure Private Access. Esta guia fornece detalhes sobre as funções suportadas para o Secure Private Access, dando aos administradores um local central para acessar e gerenciar esses recursos.



Principais benefícios:

- Informações centralizadas: Os administradores podem ver facilmente todos os recursos de solução de problemas suportados para o Secure Private Access em um só lugar.
- Observabilidade aprimorada: A nova barra de navegação esquerda na interface do usuário do Monitor lista todos os serviços do Secure Private Access, incluindo sessões, aplicativos e postura de dispositivo do Secure Private Access, proporcionando melhor observabilidade.
- Navegação aprimorada: A guia Acesso Privado Seguro inclui hiperlinks para diferentes páginas, facilitando para os administradores navegar para vários recursos e funções.

Para obter mais informações, consulte Guia Acesso Privado Seguro no Monitor.

Visibilidade para o Serviço de Acesso Privado Seguro. Para fornecer monitoramento detalhado e visibilidade para aplicativos e usuários do Acesso Privado Seguro, o Monitor agora foi aprimorado para incluir a visibilidade da sessão do Acesso Privado Seguro. A guia **Filtros** e o **Painel** fornecem informações detalhadas da sessão do Acesso Privado Seguro.

Principais recursos:

- **Filtrar Sessões de Acesso Privado Seguro**: Agora você pode filtrar sessões de Acesso Privado Seguro na guia **Filtros** > **Sessões (Web, SaaS e TCP/UDP)**.
- **Filtrar Aplicativos de Acesso Privado Seguro**: Você também pode filtrar aplicativos de Acesso Privado Seguro na guia **Filtros** > **Aplicativos (Web, SaaS e TCP/UDP)**.
- **Falhas de Aplicativos e Sessões Ativas**: Monitore falhas de aplicativos para aplicativos web/SaaS e TCP/UDP, e visualize sessões ativas para aplicativos web/SaaS no Painel.

Para obter mais informações, consulte Visibilidade para o Serviço de Acesso Privado Seguro.

Experiência de plataforma unificada para o Citrix Monitor. O Citrix Monitor agora está alinhado com todos os outros componentes dentro do Citrix Cloud, proporcionando uma experiência de plataforma unificada. A interface do usuário foi atualizada com um visual moderno, oferecendo navegação mais fácil e melhor representação de dados. A interface aprimorada é intuitiva e projetada para ajudar os usuários a compreender facilmente os dados necessários para monitorar e solucionar problemas de sessões Citrix.

Aprimoramento da guia Conexões. A guia **Conexões** agora oferece navegação simplificada para solução de problemas mais rápida. Na guia **Filtros** > página **Conexões**, você pode acessar diretamente:

- **Gerenciador de Atividades**: Clique em **Usuário Associado** ou **Nome do endpoint** para visualizar os detalhes respectivos do Gerenciador de Atividades.
- **Página Detalhes da Máquina**: Clique em **Nomes das Máquinas** para ver informações abrangentes da máquina, incluindo detalhes da máquina, detalhes de utilização, detalhes da infraestrutura e hotfixes aplicados. Para obter mais informações, consulte Solucionar problemas de máquinas. Este aprimoramento simplifica a navegação, permitindo uma resolução mais rápida de problemas relacionados à conexão.

Para obter mais informações, consulte Filtrar dados para solucionar falhas.

Filtrar detalhes de localização de recursos. Agora você pode visualizar a localização de recursos para máquinas OS de sessão única ou multi-sessão na guia **Filtros** > **Máquinas**. Este aprimoramento permite identificar e resolver rapidamente problemas relacionados a localizações de recursos específicas, levando a uma experiência de usuário mais fluida.

Para exibir a nova coluna **Localização do Recurso**, vá para **Escolher Colunas** e selecione **Localização do Recurso** na guia **Filtros** > **Máquinas**.

Aprimoramento da guia Desempenho da Sessão. A seção **Topologia da Sessão** da guia **Desempenho da Sessão** foi aprimorada para incluir as seguintes métricas de endpoint que existem no aplicativo Citrix Workspace para Windows, Mac, Linux, HTML5 ou Chrome:

- Endereço IP público
- Provedor de Serviços de Internet
- Localização, como país ou cidade
- Se a sessão do aplicativo Citrix Workspace é aberta em aplicativo nativo ou navegador (HTML5)

- Acessado usando Workspace ou StoreFront
- Utilização de recursos, como CPU %, Memória % e GPU (Total %)
- Latência da rede

Este aprimoramento ajuda a solucionar problemas relacionados a sessões rapidamente. Para obter mais informações, consulte Métricas de Desempenho da Sessão.

Uso ativo líquido da máquina. A página **Dimensionamento de carga de trabalho** agora inclui insights detalhados sobre o uso ativo líquido da máquina, fornecendo os seguintes detalhes:

- Porcentagem de uso ativo líquido
- Tempo médio de atividade da máquina
- Tempo sem sessão
- Tempo ocioso
- Tempo desconectado

Este recurso permite que você veja informações detalhadas de uso da máquina, permitindo otimizar os custos de acordo.

Para obter mais informações, consulte Dimensionamento de carga de trabalho.

Monitoramento de integridade do Cloud Connector. O componente Cloud Connector agora foi adicionado ao painel **Monitoramento de Infraestrutura**. Os Cloud Connectors são automaticamente integrados quando uma conexão entre o Citrix Cloud e seus locais de recursos é estabelecida.

Este recurso permite que os administradores monitorem a integridade dos Cloud Connectors usando uma única visualização de painel e configurem alertas proativamente.

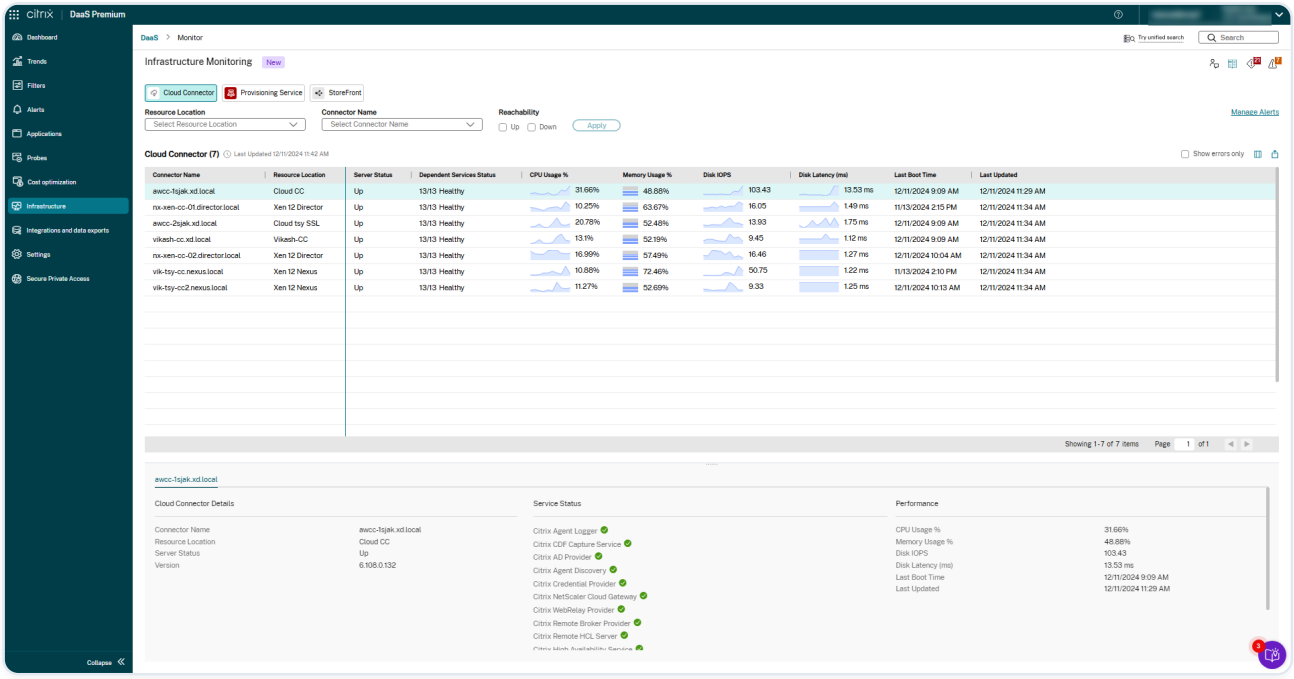
> **Nota**:
>
> O `citrixinframonitor.msi` não é necessário para monitorar os Cloud Connectors.

> **Benefícios**:

- **Monitoramento abrangente**: Visibilidade dos indicadores críticos de integridade para o Cloud Connector, como alta disponibilidade, troca de concessão de conexão e provedor AD, e assim por diante

- **Alertas configuráveis**: Você pode configurar alertas sobre métricas de integridade de interesse, definir a severidade e os escopos para que os administradores recebam alertas detalhados de acordo com a configuração do alerta.

Para monitorar o Cloud Connector, clique na guia **Infraestrutura** em Monitor. A página **Monitoramento de Infraestrutura** é aberta.



Você também pode visualizar os detalhes do status de todos os serviços na seção **Detalhes do Cloud Connector**. Para obter mais informações, consulte Métricas de integridade do Cloud Connector.

Suporte para criação de catálogos do Citrix Provisioning em ambientes VMware usando o Studio. Com o Studio, agora você pode criar catálogos do Citrix Provisioning em ambientes VMware. Anteriormente, você precisava alternar entre diferentes consoles para provisionar e gerenciar esses catálogos. Este recurso simplifica o processo, permitindo que você execute tarefas de provisionamento e gerenciamento de energia inteiramente dentro do Studio. Para obter mais informações, consulte Criar um catálogo do Citrix Provisioning em ambiente VMware usando o Studio.

Entrega de discos de anexação de aplicativos como CimFS. Anteriormente, apenas a entrega de discos de anexação de aplicativos como discos virtuais (VHD e VHDX) era suportada. Com este recurso, a entrega de discos de anexação de aplicativos como Composite Image File System (CimFS) também é suportada. Para obter informações, consulte Armazenar pacotes de aplicativos em compartilhamentos de rede.

Otimize o balanceamento de carga de armazenamento com o método de menor carga. Anteriormente, o Machine Creation Services™ (MCS) usava um método round-robin para distribuir VMs entre os repositórios de armazenamento, muitas vezes levando a uma utilização de armazenamento desigual.

O Studio agora apresenta a opção **Otimizar balanceamento de carga de armazenamento com método de menor carga**. Se você selecionar dois ou mais locais de armazenamento de dados do SO durante a criação do catálogo, esta opção ficará disponível, permitindo que os discos sejam alocados para o repositório de armazenamento menos carregado.

Este recurso aprimora o balanceamento de carga e melhora a estabilidade do sistema, e é suportado em ambientes de virtualização XenServer, VMware e SCVMM. Para obter mais informações, consulte Etapa 3. Seleção de armazenamento.

O Autoscale liga VMs hibernadas. Com este recurso, no Azure, o autoscale pode ligar VMs hibernadas de sessão múltipla do Remote Desktop Services (RDS) e VMs de sessão única compartilhadas sem sessões durante o horário de pico. As VMs podem ser de catálogos de máquinas MCS e não MCS.

Suporte para SKUs somente NVMe no Azure. Anteriormente, o MCS suportava apenas o tipo de controlador de armazenamento SCSI. Com este recurso, o MCS também suporta o tipo de controlador de armazenamento NVMe para dar suporte às novas SKUs de VM no Azure. Para obter informações sobre NVMe, consulte a documentação da Microsoft Perguntas frequentes gerais sobre NVMe. Para obter informações sobre como criar um catálogo de máquinas MCS usando uma oferta de serviço que:

- suporta SCSI e NVMe, consulte Criar um catálogo usando uma oferta de serviço que suporta SCSI e NVMe
- suporta apenas NVMe, consulte Criar um catálogo usando uma oferta de serviço que suporta apenas NVMe

Defina um fuso horário padrão para o seu site Citrix DaaS. Com o Studio, agora você pode definir um fuso horário padrão para o seu site Citrix DaaS. Para concluir esta tarefa, vá para **Configurações > Data e Hora**. O Studio usa este fuso horário para todas as exibições de tempo e agendamento, como reinício agendado e dimensionamento automático. Essa configuração facilita o gerenciamento do tempo e garante a consistência do tempo em todo o seu site. Para obter mais informações, consulte Configuração do fuso horário.

Se necessário, você pode alterar o fuso horário para recursos individuais. Por exemplo, você pode definir um fuso horário diferente para um grupo de entrega que atende máquinas em uma região

diferente. Para obter mais informações, consulte Alterar configurações do usuário em um grupo de entrega.

O Studio se alinha à experiência de navegação unificada do Citrix Cloud. Como parte da mudança para uma experiência de navegação unificada em toda a plataforma Citrix Cloud, atualizamos o Studio para se alinhar a esta iniciativa em toda a plataforma. As principais mudanças incluem um fundo verde para o painel de navegação e navegação por trilha para facilitar o acesso. Essas atualizações aprimoram a usabilidade e impulsionam a adoção de recursos, tornando mais fácil descobrir e gerenciar recursos. Para obter mais informações, consulte Studio.

Suporte para provisionamento sob demanda da AWS. Anteriormente, quando você desligava uma VM não persistente na AWS, o disco do SO não era excluído. Agora, com o provisionamento sob demanda, o disco do SO é excluído quando você desliga uma VM não persistente. Esta implementação do provisionamento sob demanda da AWS economiza custos quando a VM não está em uso. Para obter mais informações, consulte Provisionamento sob demanda da AWS.

Mostrar configurações padrão seguras. Este recurso mostra a configuração padrão segura juntamente com a configuração padrão para uma política. A configuração padrão pode ser sobrescrita pela configuração padrão segura. Se a configuração padrão segura estiver habilitada, durante a instalação do VDA, a prioridade das configurações da política é afetada da seguinte forma:

- A configuração personalizada tem a maior prioridade
- A configuração padrão segura tem a segunda prioridade
- A configuração padrão tem a menor prioridade

Para obter mais informações, consulte Configurações de política.

Exibindo detalhes da política em Eventos de Postura do Dispositivo. Agora você pode visualizar os detalhes da avaliação da política de Postura do Dispositivo como parte dos eventos de Postura do Dispositivo no Citrix DaaS Monitor. Os diferentes estados da avaliação da política e os códigos de erro são exibidos. Esse recurso simplifica a triagem e a solução de problemas do usuário. Para obter mais informações, consulte a página Diagnosticar falha de eventos de Postura do Dispositivo.

Novembro de 2024

Recursos novos e aprimorados

O gerenciamento de imagens agora está geralmente disponível. A funcionalidade de gerenciamento de imagens agora está geralmente disponível para ambientes de virtualização Azure e VMware. Além disso, o nó **Imagens** agora permite que você compartilhe versões de imagens entre unidades de hospedagem dentro da mesma conexão de hospedagem no Azure. Essa implementação garante a consistência e a uniformidade das imagens em diferentes unidades de host, aprimorando a flexibilidade de implantação e a eficiência operacional. Você também pode usar comandos PowerShell para atingir esse objetivo. Para obter mais informações, consulte Gerenciamento de Imagens.

Comunicação WebSocket. Com esse recurso, você pode configurar uma conexão WebSocket para comunicação entre VDAs e Delivery Controllers como uma alternativa ao uso da comunicação WCF. Para obter mais informações, consulte Comunicação WebSocket entre VDA e Delivery Controller.

Suporte do Studio para um snapshot do disco ou uma imagem do SO do disco como uma imagem mestre no GCP. No ambiente de virtualização do GCP, agora você pode selecionar um snapshot do disco ou uma imagem do disco como uma imagem mestre ao usar o Studio para criar um catálogo de máquinas MCS. O snapshot do disco ou uma imagem do disco pode ser regional e multirregional em comparação com a instância de VM que é apenas regional. Esse recurso simplifica significativamente o fluxo de trabalho de gerenciamento de imagens e reduz o tempo e o esforço necessários para o gerenciamento de imagens no GCP. Para obter informações sobre como criar um catálogo MCS no GCP usando o Studio, consulte Criar um catálogo de máquinas.

Conectando componentes Citrix da UI. Os administradores podem usar a UI do Monitor para registrar seus componentes Citrix para Monitoramento de Infraestrutura. Após a instalação `Citrixinframonitor.msi`, o fluxo de trabalho baseado em UI pode ser usado para concluir o processo de registro sem a necessidade de usar comandos PowerShell. Esse aprimoramento simplifica o processo de registro, cancelamento de registro e atualização de componentes Citrix.

A nova página **Conectar componentes Citrix** permite gerenciar conexões entre componentes Citrix e o site Citrix DaaS. Você também pode visualizar as conexões disponíveis do Provisioning Service e do StoreFront nesta página.

Essas atualizações simplificam o gerenciamento e a integração dos componentes Citrix, tornando mais fácil manter e monitorar sua infraestrutura.

Para obter mais informações, consulte Etapa 2: Registrar o Citrix Infrastructure Monitor na UI do Monitor.

Aprimoramento das Políticas de Alerta Avançadas. Os alertas relacionados ao Monitoramento de Infraestrutura, anteriormente conhecidos como políticas de Infraestrutura, agora fazem parte das políticas de alerta avançadas.

Você pode selecionar os serviços dependentes com base na fonte de dados selecionada e criar alertas para Cloud Connectors também.

> **Nota:**
>
> As políticas de Infraestrutura existentes criadas para Provisioning Service e StoreFront são migradas para a seção de políticas de alerta avançadas.

> Para obter mais informações, consulte Políticas de alerta avançadas.

Suporte para configurar a lista de VMs secundárias para escalar ou reduzir catálogos criados por MCS no Azure. O Web Studio agora permite que os administradores definam VMs secundárias para escalar e reduzir os catálogos criados por MCS no Azure. Com base no uso de recursos de CPU e memória, se o uso de CPU ou memória exceder um determinado limite, o sistema usará automaticamente as VMs secundárias para manipular a carga. Alternativamente, se o uso cair abaixo de um certo nível, o sistema desligará automaticamente algumas VMs para conservar recursos. Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Studio.

Detalhes do grupo de entrega aprimorados com informações de política. Aprimoramos a visualização de **Detalhes** para Grupos de Entrega adicionando uma guia dedicada que mostra as políticas atribuídas ao grupo selecionado. Essa melhoria simplifica o gerenciamento, a configuração e a solução de problemas de políticas para grupos de entrega, fornecendo acesso rápido a informações de política relevantes.

Suporte para snapshot multirregional do disco ou uma imagem do disco como imagem mestre no GCP. Um snapshot ou uma imagem de um disco no GCP pode ser regional ou multirregional. Snapshots regionais e imagens de disco estão vinculados a uma região específica, exemplo, `us-central1`, enquanto snapshots multirregionais e imagens de disco estão vinculados a uma localização geográfica, exemplo, `US`. Com este recurso, você pode usar um snapshot multirregional do disco do SO ou uma imagem do disco como entrada de imagem

mestre ao criar catálogos de máquinas MCS no GCP. Você pode ver a lista de todos os snapshots (regionais e multirregionais) em `snapshots.folder` localização e imagens de disco (regionais e multirregionais) em `images.folder` no caminho do inventário da unidade de hospedagem.

Suporte para converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil em ambiente VMware. No ambiente VMware, agora você pode usar um modelo VMware como entrada de perfil de máquina para converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil. Novas VMs adicionadas ao catálogo assumem os valores de propriedade do perfil da máquina. Para obter mais informações, consulte Converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil.

Suporte para Windows Server 2025. O Citrix Virtual Apps and Desktops agora oferece suporte ao Windows Server 2025. Para obter mais informações sobre o Windows Server 2025, consulte a documentação da Microsoft Novidades no Windows Server 2025.

Studio: Suporte para provisionamento de VMs persistentes no SO Windows Server usando Full Copy Clone. O Studio agora oferece suporte ao provisionamento de VMs persistentes no SO Windows Server usando a abordagem Full Copy Clone. Essa abordagem melhora os recursos de recuperação e migração de dados e pode ajudar a reduzir as IOPS após a criação das máquinas. Para obter mais informações, consulte Selecionar uma experiência de desktop e Modo de cópia de máquina virtual.

Studio AWS Quick Deploy: Suporte para adicionar contas AWS não habilitadas para BYOL. O Studio agora permite que você conecte uma conta AWS sem habilitar o recurso BYOL para uma região. Você pode configurar o recurso BYOL para uma região posteriormente. A conta sem BYOL habilitado para uma região tem a restrição de selecionar apenas imagens de tenancy padrão e conexão de diretório compartilhado para continuar a configurar a conta. Para obter mais informações, consulte Conectar sua conta AWS.

Backup e restauração usando o Studio agora estão geralmente disponíveis. Agora você pode usar o nó Backup e Restauração disponível no painel esquerdo do seu console Manage DaaS. Este recurso permite criar backups sob demanda e agendados e restaurar aplicativos, políticas e muito mais excluídos. Para obter mais informações, consulte Backup e Restauração usando o Studio.

Widget de guias de configuração na página inicial do Studio. Atualizamos a página **Home** do Studio renomeando o widget **Introdução** para **Guias de configuração**. Este widget agora inclui o guia original **Introdução ao DaaS** e um novo guia **Verificar configurações de resiliência**.

Guia de verificação de configurações de resiliência. Introduzimos um novo guia **Verificar configurações de resiliência** no widget **Guias de configuração** na página **Home** do Studio. Este guia fornece listas de verificação para verificar as configurações de resiliência em vários tipos de implantações do StoreFront:

- Lista de verificação para implantações do StoreFront no local
- Lista de verificação para implantações do Citrix® StoreFront Cloud
- Lista de verificação para implantações mistas do StoreFront

Seguindo este guia, você pode verificar se o Local Host Cache e a Continuidade do Serviço estão configurados corretamente em sua implantação, garantindo acesso ininterrupto a aplicativos e desktops durante interrupções de serviço.

Guia de introdução ao DaaS agora geralmente disponível. O **Guia de introdução ao DaaS** otimiza e simplifica o processo de implantação do DaaS para administradores novos e experientes. Este guia o orienta na configuração de sua implantação DaaS, fazendo uma série de perguntas para guiar a configuração. Para obter mais informações, consulte Usar o guia de introdução ao DaaS.

Seleção de domínio aprimorada. Uma nova opção na interface do usuário agora permite que você insira um nome de domínio para uma correspondência exata sempre que a seleção de domínio for necessária. Este aprimoramento oferece os seguintes benefícios:

- Pesquisas mais rápidas: Você pode pular a navegação em grandes diretórios, obtendo resultados direta e instantaneamente.
- Economia de tempo: Elimina o carregamento completo do diretório, acelerando os fluxos de trabalho.
- Experiência aprimorada: Melhora a eficiência do gerenciamento do administrador, especialmente em ambientes com grandes diretórios.

Validar a configuração antes de criar um catálogo de máquinas MCS em ambientes AWS. Com este recurso, agora você pode validar as configurações antes de criar um catálogo de máquinas MCS em ambientes AWS usando o parâmetro `-validate` no comando `New-ProvScheme`. Depois de executar este comando PowerShell com o parâmetro, você receberá uma mensagem de erro apropriada se houver um parâmetro incorreto usado ou se um parâmetro entrar em conflito com outro. Você pode então usar a mensagem de erro para resolver o problema e criar com sucesso um catálogo de máquinas MCS usando o PowerShell. Este recurso é

aplicável a ambientes de virtualização AWS, Azure, GCP e VMware. Para obter mais informações, consulte Validar a configuração antes de criar um catálogo de máquinas MCS.

Atualização do painel de Métricas de Desempenho. O painel **Métricas de Desempenho** possui uma visualização aprimorada das métricas de dados históricos. Ao clicar na guia **Desempenho da Sessão**, juntamente com os dados dos últimos 15 minutos, você pode visualizar os dados das últimas 48 horas para ICARTT e Latência ICA®. Este aprimoramento ajuda a reduzir o tempo médio de resolução, permitindo que os administradores resolvam problemas mesmo que a sessão tenha sido encerrada nas últimas 48 horas.

Para obter mais informações, consulte a seção Métricas de desempenho.

Aprimoramento da guia Filtros. Com esta versão, os seguintes filtros adicionais são adicionados à guia **Sessões**.

- **Todos** - Exibe todas as sessões
- **Ativas, Conectadas e Desconectadas** - Exibe apenas as sessões ativas, conectadas e desconectadas.
- **Encerradas** - Exibe apenas as sessões que foram encerradas nas últimas 48 horas. O filtro padrão é **Ativas, Conectadas e Desconectadas**.

Aprimoramento da sessão encerrada . Na sessão encerrada (anteriormente sessão histórica), a guia **Desempenho da Sessão** mostra dados das últimas 48 horas. Além disso, você pode visualizar a guia **Logon da Sessão** para a sessão encerrada.

Para obter mais informações, consulte a página Diagnosticar sessões de usuário encerradas [Visualização].

Outubro de 2024

Recursos novos e aprimorados

Conjuntos de políticas agora geralmente disponíveis. Conjuntos de políticas são coleções de regras e diretrizes que permitem operações de gerenciamento simplificadas, baseadas em função e fáceis. Os conjuntos de políticas permitem criar divisões lógicas dentro de sua equipe de administradores, organizações ou máquinas. Você pode atribuir escopos e grupos de entrega para que administradores autorizados possam gerenciar as políticas relevantes para usuários e máquinas. Para obter mais informações, consulte Conjuntos de políticas.

Registrar máquinas persistentes do tipo híbrido ingressado no Azure AD no Microsoft Intune para cogestão. Durante a criação do catálogo de máquinas, agora você pode registrar máquinas persistentes do tipo híbrido ingressado no Azure AD no Microsoft Intune (com Configuration Manager) para cogestão. Esse recurso se aplica a VMs persistentes de sessão única e multi-sessão e em todos os hipervisores e serviços de nuvem, garantindo um gerenciamento uniforme de dispositivos em toda a sua infraestrutura. Este recurso é aplicável apenas à versão 2407 do VDA e posterior.

Para obter mais informações, consulte Catálogos híbridos ingressados no Azure AD registrados no Microsoft Intune e Criar catálogos híbridos ingressados no Azure AD registrados no Microsoft Intune.

Diagnosticar falhas de autenticação condicional. Sempre que qualquer autenticação condicional falhar, você pode usar o ID da transação disponível na mensagem de falha e pesquisar no Monitor os detalhes da falha. O Monitor ajuda você a solucionar eventos de falha de autenticação condicional exibindo os motivos da falha e as políticas condicionais na interface do usuário do Monitor. Para obter mais informações, consulte Diagnosticar falhas de autenticação condicional.

Contas de serviço para gerenciamento de identidade de máquina. O MCS desenvolveu um novo mecanismo para gerenciar contas de serviço de identidade do Active Directory local e do Azure Active Directory (Azure AD) para simplificar e aprimorar o gerenciamento de identidades de máquina, incluindo contas de computador no Active Directory local, dispositivos ingressados no Azure AD e dispositivos registrados no Intune. Primeiramente, introduzimos o suporte a contas de serviço do Active Directory local, que permite aos administradores gerenciar contas de computador no Active Directory local sem precisar inserir credenciais de domínio a cada vez. Em segundo lugar, introduzimos o suporte a Nomes de Entidade de Serviço (SPN) de identidade do Azure AD, que permite aos administradores gerenciar dispositivos ingressados no Azure AD ou registrados no Intune no locatário do Azure AD, de forma segura e simplificada. Por fim, implementamos um novo mecanismo para gerenciamento de contas de serviço em nosso Studio, simplificando o processo e facilitando a manutenção da segurança e conformidade. Para obter mais informações, consulte Contas de serviço para gerenciamento de identidade de máquina.

Suporte para selecionar um modelo de instância como perfil de máquina. Ao criar catálogos de máquinas MCS em ambientes GCP usando o Studio, agora você pode selecionar Modelos de Instância como entradas para perfis de máquina. Além disso, as configurações da Chave de Criptografia Gerenciada pelo Cliente (CMEK) seguem uma sequência de prioridade. Para obter mais informações, consulte Criar um catálogo de máquinas usando o Studio

Exportar um perfil de máquina para uma especificação de modelo ARM. O Studio agora oferece suporte à exportação do perfil de máquina usado por um catálogo para uma especificação de modelo ARM. Com esse recurso, você pode reutilizar facilmente um perfil de máquina existente como um modelo e modificá-lo para futuras necessidades de provisionamento. Para obter mais detalhes, consulte Exportar um perfil de máquina como uma especificação de modelo ARM.

Catálogos MCS: suporte a modelos de inicialização AWS. Agora você pode usar modelos de inicialização AWS como perfis de máquina ao criar ou editar catálogos MCS em seu ambiente AWS. Os modelos de inicialização AWS estão disponíveis na lista de perfis de máquina para seleção.

Recuperar informações do Connector Appliance. Com este recurso, você pode usar o comando PowerShell `Get-ConfigEdgeServer` para recuperar as informações do Connector Appliance.

- `Get-ConfigEdgeServer -ConnectorType 'Unified'`: Retorna informações do Connector Appliance
- `Get-ConfigEdgeServer -ConnectorType 'Windows'`: Retorna apenas informações de servidores de borda
- `Get-ConfigEdgeServer`: Retorna apenas informações de servidores de borda.

Agendamentos de reinicialização para VMs hibernadas. Com este recurso, você pode configurar agendamentos de reinicialização para VMs hibernadas se o Grupo de Entrega estiver habilitado para hibernação. No ciclo de reinicialização, as VMs são retomadas e, em seguida, desligadas. O agendamento de reinicialização pode ser definido como semanal, diário, mensal e uma vez. Você pode configurar vários agendamentos. Observe que as VMs que são retomadas da hibernação podem levar alguns minutos.

Cache de dados para o nó Imagens. Introduzimos o cache de dados para o nó **Imagens** para melhorar a experiência geral do usuário. Esse aprimoramento reduz significativamente o tempo de carregamento da página quando você navegar para as listas **Definição de imagem** e **Versões de imagem**, bem como as guias **Detalhes** e **Esquema de imagem**.

Rotulagem de logs de configuração. Agora você pode rotular logs de configuração na guia **Logs > Eventos**, facilitando a identificação e exportação de logs. Além disso, o nó **Registro em log** agora oferece recursos aprimorados, incluindo exportação de logs para arquivos CSV, pesquisa avançada e exibição em estilo de tabela para a guia **Eventos**. Para obter mais informações, consulte Exibir conteúdo do log de configuração.

Suporte para criar uma conexão de host usando a Identidade Gerenciada do Azure. Anteriormente, você podia criar uma conexão de hospedagem do Azure usando uma entidade de serviço. Isso exigia o fornecimento e o armazenamento do ID do aplicativo e do segredo da entidade de serviço. As Identidades Gerenciadas do Azure oferecem uma maneira segura e escalável de acessar os serviços do Azure sem a necessidade de gerenciar credenciais. Essa abordagem elimina os riscos associados ao armazenamento, rotação e gerenciamento de segredos. As identidades gerenciadas também suportam a atualização automática de tokens, garantindo que os aplicativos sempre usem credenciais válidas sem nenhum código adicional para o gerenciamento do ciclo de vida do token.

Com este recurso, você pode criar uma conexão de host com o Microsoft Azure Resource Manager usando a Identidade Gerenciada do Azure. Atualmente, você pode criar a conexão de host usando apenas comandos do PowerShell. Para obter informações sobre como criar uma conexão de host usando a Identidade Gerenciada do Azure, consulte Criar uma conexão de host usando a Identidade Gerenciada do Azure.

Suporte para Monitoramento de Integridade de Inicialização no Azure. Com este recurso, em ambientes de virtualização do Azure, você pode habilitar o Monitoramento de Integridade de Inicialização para VMs de catálogo de máquinas MCS (VMs persistentes e não persistentes) usando um perfil de máquina (VM ou especificação de modelo) que tenha a extensão GuestAttestation instalada. O Monitoramento de Integridade de Inicialização é suportado apenas para Inicialização Confiável e VMs Confidenciais que usam Inicialização Segura e Módulo de Plataforma Confiável virtual (vTPM).

Se sua VM tiver Inicialização Segura e vTPM habilitados, e a extensão GuestAttestation instalada, o Microsoft Defender for Cloud pode validar remotamente se sua VM inicializa corretamente. Esse monitoramento é chamado de Monitoramento de Integridade de Inicialização. Para obter mais informações sobre o monitoramento de integridade de inicialização, consulte Visão geral do monitoramento de integridade de inicialização.

Para obter informações sobre como criar um catálogo habilitado com monitoramento de integridade de inicialização, consulte Monitoramento de Integridade de Inicialização.

Filtrar grupos de recursos vazios. Com este recurso, você pode filtrar grupos de recursos vazios ao selecionar uma imagem mestre, perfil de máquina ou imagem preparada durante a criação do catálogo de máquinas. Você pode fazer isso usando um comando PowerShell `Get-HypInventoryItem`. Para obter mais informações, consulte Filtrar grupos de recursos vazios.

Suporte para criação de catálogos de disco WBC pré-formatados no Azure. Com este recurso, em ambientes de virtualização do Azure, você pode utilizar um disco WBC pré-formatado para catálogos recém-criados. Essa ação reduz significativamente o tempo necessário para iniciar cada VM de um catálogo de máquinas MCS ou Citrix Provisioning™ provisionado por MCS. Para implementar essa funcionalidade, crie um catálogo do Azure com WBC habilitado e inclua uma propriedade personalizada adicional `PreformatWriteBackCache` como `True`.

Você pode atualizar um catálogo existente usando o comando `Set-ProvScheme` para atualizar o tamanho do disco WBC.

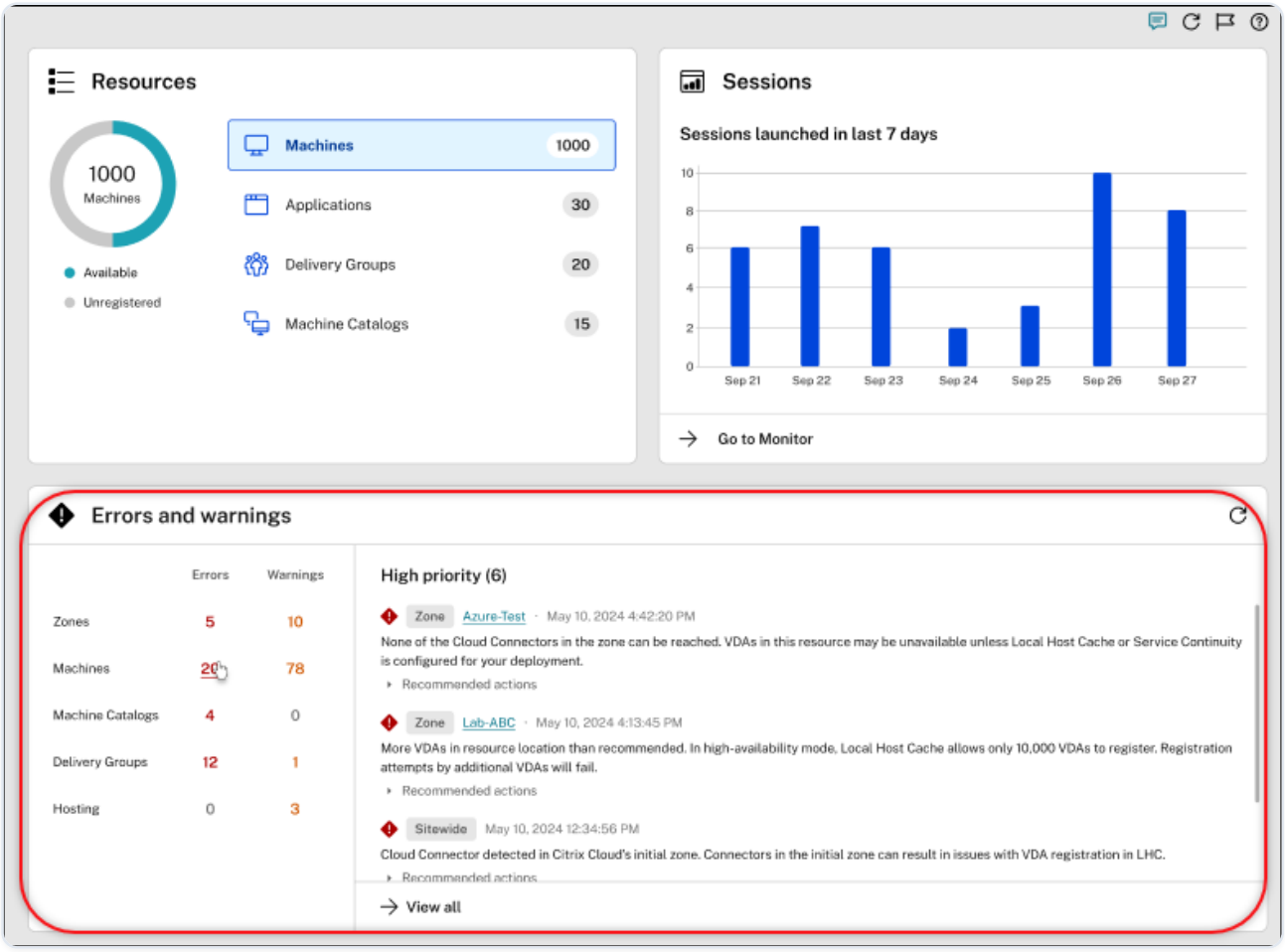
Este recurso é compatível com o fluxo de trabalho de gerenciamento de imagens, onde o MCS separa a fase de masterização do fluxo de trabalho geral de provisionamento. Para obter mais informações, consulte Criar um catálogo de disco WBC pré-formatado.

Excluir disco WBC no desligamento para catálogos Citrix Provisioning provisionados por MCS. Com este recurso, você tem a opção de excluir o disco de cache de gravação (WBC) depois de desligar a VM para catálogos Citrix Provisioning provisionados por MCS no Azure. Essa implementação ajuda a economizar custos quando você não precisa de um disco WBC persistente. Este recurso também é aplicável a um catálogo existente. Para obter mais informações, consulte Excluir disco WBC no desligamento para catálogos Citrix Provisioning provisionados por MCS.

Suporte para criação de um grupo de segurança de rede. Com este recurso, agora você pode criar um grupo de segurança de rede Deny-All para preparação de imagem, em vez de solicitar que a Citrix crie e modifique um grupo de segurança de rede automaticamente. Edite as propriedades personalizadas da unidade de hospedagem usando um comando PowerShell `Set-Item` para incluir o parâmetro `NsgForPreparation` para fornecer o grupo de segurança de rede Deny-All. Para obter mais informações sobre como usar o comando PowerShell, consulte Usar um grupo de segurança de rede pré-criado.

Suporte para usar disco temporário do Azure como disco WBC para catálogos de máquinas MCS existentes. Com este recurso, agora você pode usar o disco temporário do Azure como um disco de cache de gravação (WBC) para catálogos de máquinas MCS existentes e VMs existentes. Use o comando PowerShell `Set-ProvScheme` para atualizar os catálogos existentes. Essa implementação economiza custos de armazenamento porque o disco temporário do Azure é gratuito. Para obter informações sobre as etapas, consulte Usar disco temporário como disco WBC para catálogos existentes.

Central de erros e avisos. Com um novo widget, **Erros e avisos**, na página **Início** do Studio, agora você pode visualizar todos os erros e avisos de suas implantações DaaS em um só lugar. Este widget simplifica a resolução de problemas, consolidando alertas dispersos, aumentando a visibilidade e reduzindo o tempo de solução de problemas. Para obter mais informações, consulte Página inicial.



Melhoria na página Tendências. A página **Tendências** agora apresenta dois novos banners que levam à página **Otimização de custos**, proporcionando acesso mais rápido a informações e relatórios de economia de custos. A guia **Uso da Máquina** agora inclui links para **Economias Estimadas** e **Relatório de Economias**, enquanto a guia **Utilização de Recursos** oferece um link para **Dimensionamento de carga de trabalho** (anteriormente conhecido como **Dimensionamento de infraestrutura**). Essas melhorias simplificam a navegação e aprimoram a visibilidade, permitindo que os usuários tomem decisões baseadas em dados para otimização de custos. Para obter mais informações, consulte a página Tendências.

Setembro de 2024

Recursos novos e aprimorados

Backup e restauração usando o Studio (Preview). Agora você pode usar o nó **Backup e Restauração** disponível no painel esquerdo do seu console Gerenciar DaaS. Este recurso permite criar backups sob demanda e agendados e restaurar aplicativos, políticas e muito mais que foram excluídos. Para obter mais informações, consulte Backup e restauração usando o Studio (Preview).

Validar permissões na conexão do host no Azure. Anteriormente, em ambientes Azure, você podia validar apenas as credenciais de conexão do host (ID do cliente ou ID do aplicativo) usadas para criar uma conexão com o Azure.

Com este recurso, você pode:

- Obter a lista de permissões atribuídas à sua credencial de conexão do host
- Obter a lista de operações que podem ser realizadas com as permissões atribuídas
- Informações sobre as permissões necessárias
- Informações sobre como adicionar as permissões desejadas

Isso ajuda você a solucionar problemas e obter as permissões necessárias com antecedência para que você possa realizar as tarefas sem ser bloqueado. Para obter mais informações, consulte Validar permissões na conexão do host.

Criar catálogos do Citrix Provisioning usando comandos MCS PowerShell no XenServer. Agora você pode criar catálogos do Citrix Provisioning usando comandos MCS PowerShell em ambientes XenServer. Você pode criar catálogos do Citrix Provisioning baseados em perfil de máquina e não baseados em perfil de máquina. Para obter mais informações, consulte Criar catálogos do Citrix Provisioning no Citrix Studio.

Reparar as informações de identidade de contas de computador ativas no GCP, SCVMM e XenServer. Em ambientes GCP, SCVMM e XenServer, agora você pode redefinir as informações de identidade de contas de computador ativas que apresentam problemas relacionados à identidade. Você pode optar por redefinir apenas a senha da máquina e as chaves de confiança, ou redefinir toda a configuração do disco de identidade. Esta implementação é aplicável a catálogos de máquinas MCS persistentes e não persistentes. Atualmente, o recurso é compatível com ambientes de virtualização AWS, Azure, GCP, SCVMM, VMware e XenServer. Para obter mais informações, consulte Reparar as informações de identidade de contas de computador ativas.

Suporte para a criação de catálogos unidos ao Azure AD inscritos no Microsoft Intune para VMs não persistentes. Agora você pode criar catálogos unidos ao Azure AD inscritos no Microsoft Intune para sessões únicas e múltiplas não persistentes. Este recurso é aplicável apenas à versão 2407 do VDA e posterior.

Para obter informações sobre requisitos, limitações e considerações sobre catálogos habilitados para Microsoft Intune usando o Citrix DaaS, consulte Microsoft Intune.

Para obter informações sobre a criação de catálogos habilitados para Microsoft Intune, consulte Pool de identidade de identidade de máquina habilitada para Microsoft Intune.

Nova opção de publicação de aplicativos para associar tipos de arquivo a aplicativos. Adicionamos uma opção, **Associação de Tipo de Arquivo**, para publicar aplicativos no Studio. Este recurso permite especificar e gerenciar extensões para aplicativos ao publicá-los:

- Ao adicionar aplicativos de Acesso a Aplicativos Locais, esta opção aparece no painel esquerdo.
- Ao adicionar um aplicativo para entrega ou grupos de aplicativos, esta opção é acessível através do menu **Propriedades** do aplicativo.

Este aprimoramento garante uma experiência de publicação de aplicativos mais abrangente e simplificada.

Aprimoramentos no widget de Visualização. Aprimoramos o widget de **Visualização** no Citrix DaaS, proporcionando uma experiência de visualização mais simplificada e amigável. Os aprimoramentos incluem:

- **Registro de atividades de visualização.** A ativação ou desativação de recursos de visualização agora é registrada no nó de Log. Este recurso garante visibilidade sobre a ativação e desativação de recursos de visualização para fins de auditoria e solução de problemas.
- **Informações contextuais.** Conteúdo suplementar para recursos de visualização agora está disponível para melhorar sua compreensão de cada recurso de visualização. As informações incluem links para pacotes de instalação, vídeos de demonstração, formulários Podio, artigos de visualização, blogs e outras documentações relevantes.
- **Opção de feedback.** Com um novo ícone, **Enviar Feedback**, agora você pode fornecer diretamente feedback, comentários e sugestões para recursos de visualização. Este recurso nos ajuda a coletar informações valiosas e aprimorar nossos serviços com base em sua contribuição.

Opção para exportar dados da página de Otimização de custos. Você pode exportar os dados na página de **Otimização de custos** usando integração de dados e consultas ODATA. Para exportar dados, você pode usar uma das seguintes opções:

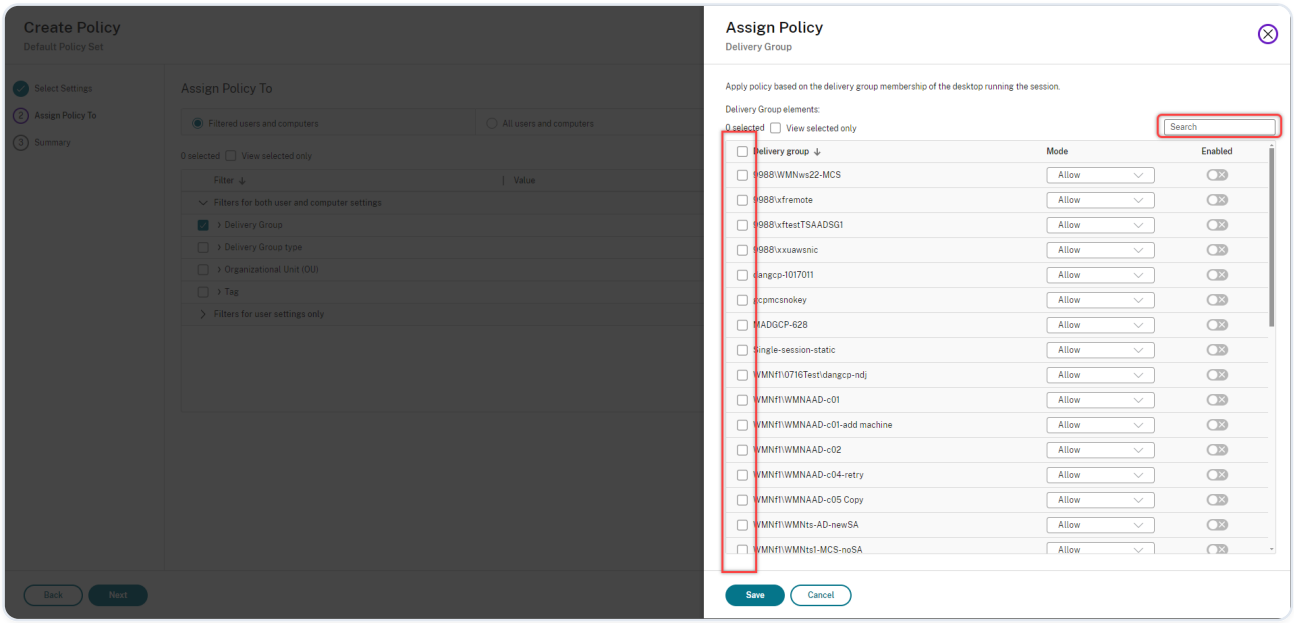
- Configurar integração de dados - Você pode integrar dados de Otimização de custos com a API do Monitor Service, através da qual você pode coletar os dados para solucionar e triar os problemas. Para obter mais informações, consulte a página Integrações e exportações de dados.
- Consultas ODATA para otimização de custos - Você pode usar as consultas ODATA de exemplo disponíveis na página de **Otimização de custos** para exportar dados.

Para obter mais informações, consulte Exportar dados.

Configuração de webhook usando o PowerShell SDK. O recurso de Configuração de Webhook usando o PowerShell SDK permite que os administradores criem, modifiquem, excluam e listem perfis de webhook. Este recurso oferece flexibilidade na configuração de webhooks, permitindo a especificação de cabeçalhos, tipos de autenticação, tipos de conteúdo, payloads e URLs de webhook.

> **Nota:**
>
> O formato de payload suportado é texto e o usuário final deve habilitar o texto em seu webhook.
>
> Para obter mais informações, consulte a documentação Configuração de webhook usando o SDK do PowerShell.

Experiência aprimorada de atribuição de política. Agora você pode simplificar suas atribuições de política no nó **Políticas** com as novas funções de multisseleção e pesquisa. Com essas funções, você pode visualizar todos os objetos de um tipo selecionado na página **Atribuir Política** e atribuir configurações de política a vários destinos em menos cliques. Você também pode usar a função de pesquisa para filtrar e encontrar rapidamente objetos específicos, economizando seu tempo e reduzindo erros.

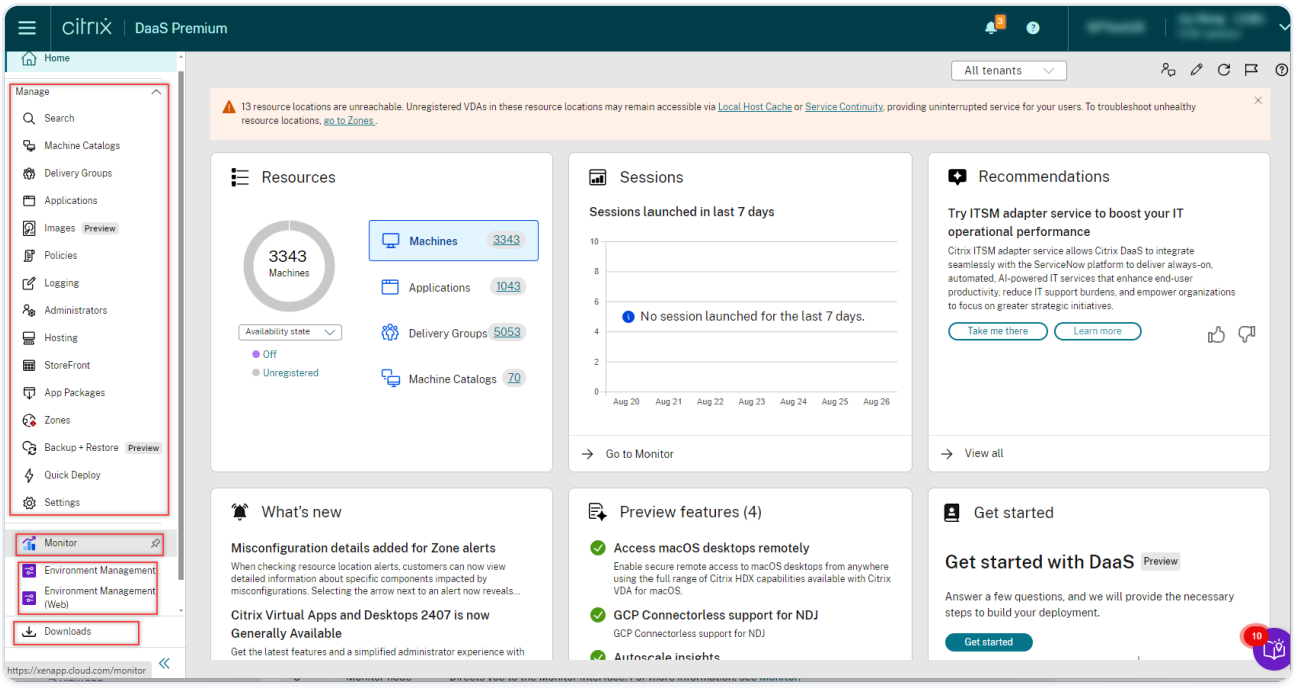


Agosto de 2024

Recursos novos e aprimorados

Painel de navegação do DaaS redesenhado. Reformulamos o painel de navegação do DaaS para otimizar suas tarefas de gerenciamento:

- **Navegação simplificada:** Reduzida de duas para uma camada, movendo os menus **Gerenciar** e **Monitorar** e o link **Downloads** da barra de menu superior para o painel de navegação esquerdo.
- **Configuração centralizada:** Todos os nós e menus relacionados à configuração agora estão localizados na seção Gerenciar no painel de navegação esquerdo, consolidando itens dos menus anteriores **Configuração Completa** e **Implantação Rápida**.
- **Serviços de nuvem reorganizados para gerenciamento de máquinas:** Os serviços **Gerenciamento de Ambiente**, **Gerenciamento de Ambiente (Web)** e **Gravação de Sessão**, anteriormente no menu **Gerenciar**, agora estão no mesmo nível do menu **Gerenciar** no painel de navegação.
- **Fixar menus para acesso rápido:** A função **Fixar** recém-adicionada permite fixar menus usados com frequência na parte superior do painel de navegação para acesso rápido. Você pode reordenar os menus fixados arrastando-os para os locais desejados.



O MCS cria discos de ID com tipo de volume GP3 no ambiente AWS. Anteriormente, em ambientes AWS, os discos de identidade (ID) das VMs eram do tipo de volume GP2. Com esse recurso, o MCS agora pode provisionar VMs com discos de identidade do tipo de volume GP3. Como o tipo de volume GP3 é a opção mais barata oferecida pela AWS, esse recurso minimiza os custos.

O recurso é aplicável apenas às VMs adicionadas a um novo catálogo e às novas VMs adicionadas a um catálogo existente. As VMs existentes criadas antes desse recurso continuam a ter discos de ID com tipo de volume GP2, a menos que o disco de ID seja redefinido.

Validar permissões na conexão do host na AWS. Em ambientes AWS, agora você pode validar permissões em uma conexão de host para realizar tarefas relacionadas à criação e gerenciamento de catálogos de máquinas MCS. Essa implementação ajuda você a descobrir as permissões ausentes necessárias para diferentes cenários, como criação, exclusão e atualização de VMs, gerenciamento de energia de VMs e criptografia EBS, com antecedência, para que você possa evitar ser bloqueado em momentos críticos. Para obter mais informações, consulte Validar permissões na conexão do host.

Criar imagem personalizada a partir de uma instância de Workspace existente. Esse aprimoramento permite criar uma imagem personalizada a partir de uma instância de workspace já existente. Para obter mais informações, consulte Criar imagem personalizada a partir de uma instância de Workspace existente.

Persistir o tipo de armazenamento BDM como SSD padrão no Azure. Doravante, para catálogos do Citrix Provisioning criados usando MCS no Azure, o tipo de armazenamento BDM é

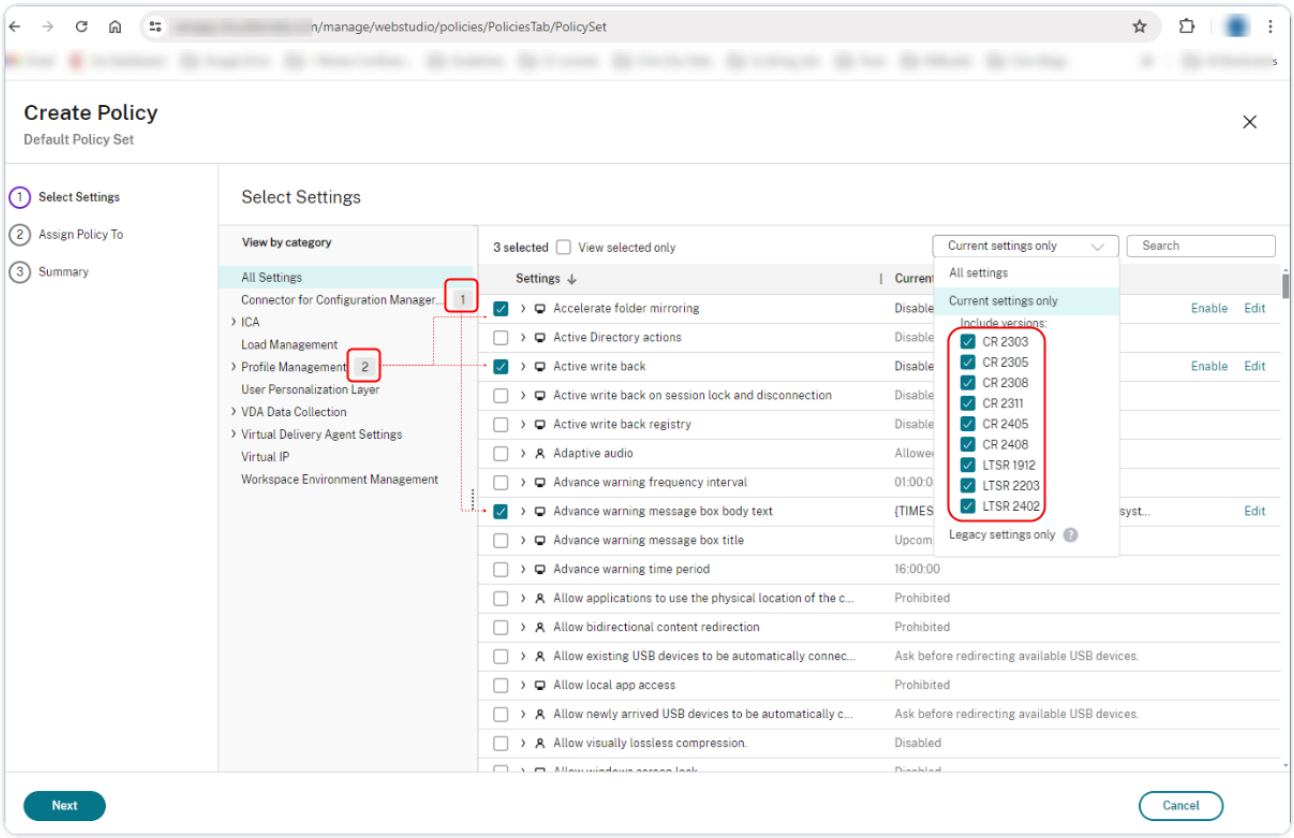
configurado como SSD padrão por padrão. Esta opção é considerada uma medida de economia de custos e não pode ser modificada.

Personalize a página inicial. Agora você pode personalizar a página **Inicial** do DaaS adicionando, removendo e reposicionando seus widgets para melhor atender às suas necessidades. Essa personalização é específica para cada administrador, garantindo uma experiência de painel personalizada. Para obter mais informações, consulte Página inicial da interface de Configuração Completa.

Detalhes de configuração incorreta adicionados para alertas de Zona. Ao verificar alertas de localização de recursos, agora você pode visualizar informações detalhadas sobre componentes específicos impactados por configurações incorretas. Anteriormente, apenas informações gerais estavam disponíveis na guia **Solução de problemas** do nó **Zonas**, dificultando a resolução de problemas precisos. Com esta melhoria, clicar na seta direcional direita ao lado de um alerta revela detalhes mais específicos, permitindo que você tome ações direcionadas sobre configurações incorretas. Para obter mais informações, consulte Solução de problemas.

Interface do usuário de Políticas aprimorada para melhor experiência do usuário. Aprimoramos o design da interface do usuário para o nó **Políticas** para melhorar sua usabilidade e funcionalidade gerais. As melhorias detalhadas incluem:

- **Tela cheia para interfaces de criação e edição.** O modo de tela cheia agora é usado para uma experiência de criação e edição aprimorada e mais eficiente no nó **Políticas**.
- **Filtragem de configurações simplificada.** Uma lista suspensa para versões VDA suportadas agora está disponível no filtro **Somente configurações atuais**, permitindo que você filtre as configurações com base nas versões VDA.
- **Categorização de configurações aprimorada.** Ao selecionar várias configurações, o número de configurações escolhidas agora aparece ao lado das categorias e subcategorias relevantes no painel esquerdo. Essa melhoria ajuda você a identificar rapidamente a categoria e as subcategorias às quais cada configuração selecionada pertence, otimizando o gerenciamento de suas políticas.



Cache de dados para a guia Detalhes nos nós de Configuração Completa. Introduzimos o cache de dados para a guia **Detalhes** em todos os nós de Configuração Completa. Essa melhoria reduz significativamente o tempo de carregamento de dados para as guias **Detalhes**, aprimorando a experiência geral do usuário.

Gráficos de monitoramento de uso de aplicativos no Painel. Agora, o Citrix Monitor ajuda você a monitorar o uso de aplicativos publicados. Este recurso está presente no Painel e contém gráficos selecionados para ajudar os administradores de TI ou administradores de aplicativos a obter informações sobre quais aplicativos são muito usados e a extensão de seu uso.

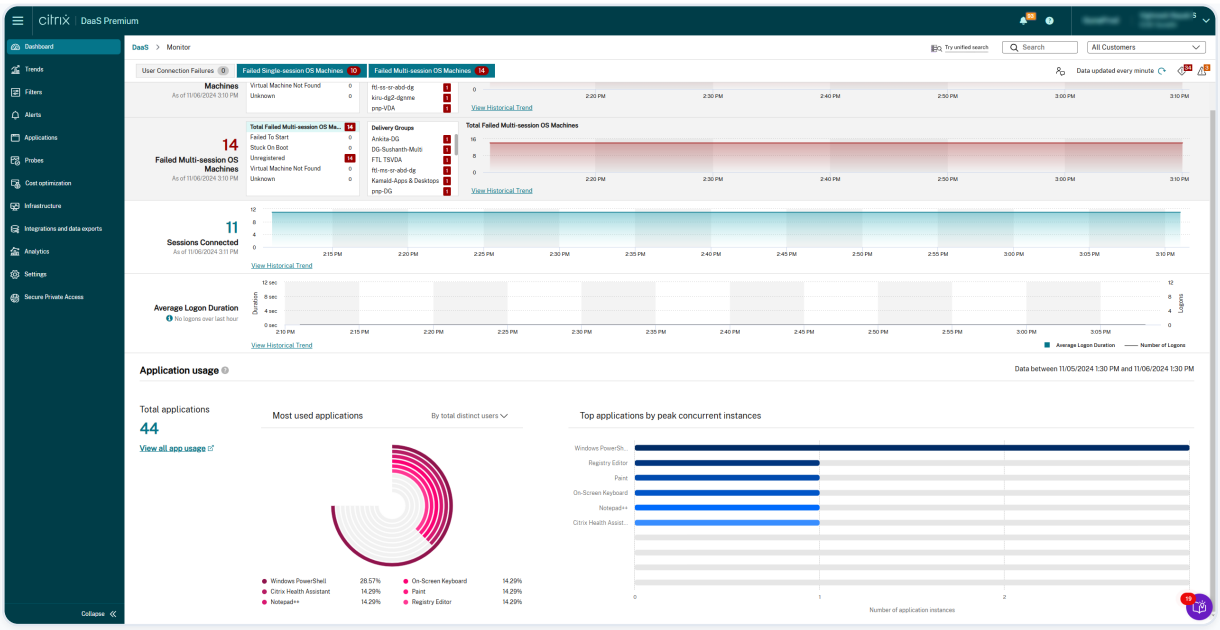
Esses gráficos compreendem os seguintes pontos de dados para as últimas 24 horas:

- Número total de aplicativos em uso
- Aplicativos mais usados (limite de 10) pelo número total de usuários distintos
- Aplicativos mais usados (limite de 10) pelo número total de inicializações de aplicativos
- Principais instâncias de aplicativos simultâneos de pico

Através desta visualização, os clientes podem ter visibilidade sobre os aplicativos publicados populares para realizar uma análise de Consumo versus Direito para otimizar o custo incorrido na compra de licenças de software.

Nota:

Este recurso está disponível apenas para sites com licença platinum.



Para obter mais informações, consulte Gráficos de monitoramento de uso de aplicativos no Painel.

Opção para visualizar e filtrar o tipo de sessão e a última hora de inicialização. O Citrix Monitor agora oferece uma opção para adicionar **Tipo de Sessão** como uma nova coluna. Os diferentes tipos de sessão disponíveis são desktop e aplicativo. Você também pode adicionar **Tipo de Sessão** como uma nova coluna adicionando-o em **Filtros** > **Sessões** > **Escolher Colunas.** Isso também é adicionado em **Tendências > Sessões.**

Da mesma forma, uma nova opção para descobrir a **Última Hora de Inicialização** é adicionada na seção **Filtros** > **Máquinas**. Você também pode adicionar **Última Hora de Inicialização** como uma nova coluna adicionando-a em **Filtros** > **Máquinas** > **Escolher Colunas**.

Converter catálogos MCS legados em catálogos baseados em perfil de máquina no Azure e AWS. Agora você pode converter catálogos de máquinas não baseados em perfil de máquina em catálogos de máquinas baseados em perfil de máquina na Configuração Completa para ambientes Azure e AWS. Essa nova capacidade permite que você atualize catálogos MCS legados para os catálogos baseados em perfil de máquina recomendados.

Para obter mais informações, consulte:

- Converter catálogos MCS legados no Azure para catálogos baseados em perfil de máquina
- Converter catálogos MCS legados na AWS para catálogos baseados em perfil de máquina

Suporte para configuração de tamanhos de VM de backup. As nuvens públicas podem, às vezes, ficar sem capacidade para um tamanho de VM específico. Além disso, se você usar VMs Spot do Azure, as VMs serão despejadas a qualquer momento com base nas necessidades de capacidade do Azure. Em tal caso de capacidade insuficiente no Azure ou falha na inicialização de uma VM Spot, o MCS agora recorre aos tamanhos de VM de backup.

Você pode fornecer uma lista de tamanhos de VM de backup usando uma propriedade personalizada `BackupVmConfiguration`. O MCS tenta recorrer aos tamanhos de VM de backup na ordem fornecida por você na lista. Caso o MCS não consiga recorrer a todos os tamanhos de VM de backup fornecidos, você receberá uma mensagem de erro. Este recurso é suportado apenas para um catálogo que usa um perfil de máquina e é aplicável a catálogos de máquinas MCS persistentes e não persistentes. Este recurso é atualmente suportado apenas para ambientes Azure. Para obter mais informações, consulte Configurar tamanhos de VM de backup.

Julho de 2024

Recursos novos e aprimorados

Configurar as permissões de conexão de host do Azure necessárias. Anteriormente, o teste de conexão do host validava se a credencial era boa para se conectar ao hipervisor. O teste não realizava a validação das permissões reais que você poderia precisar para executar operações MCS relevantes, como gerenciamento de energia, criação de VM e muitas outras.

Com este recurso, agora você pode configurar facilmente todas as permissões mínimas necessárias para um principal de serviço ou conta de usuário no Azure, vinculado a uma conexão de host, para executar todas as operações MCS usando um modelo ARM. Este modelo ARM automatiza o seguinte:

- Criação de uma Função do Azure com permissões mínimas necessárias para as operações.
- Atribuição desta função a um Principal de Serviço do Azure existente no nível da assinatura.

Você pode implantar este modelo ARM usando o Portal do Azure ou comandos do PowerShell. Para obter mais informações, consulte Modelo ARM para Operações CVAD.

Painel de Métricas de Desempenho Aprimorado. O painel **Métricas de Desempenho** possui uma visualização aprimorada das métricas de dados históricos. Ao clicar na guia **Desempenho da Sessão**, juntamente com os dados dos últimos 15 minutos, você pode visualizar os dados das últimas 24 horas para ICARTT e Latência ICA. Este aprimoramento ajuda a reduzir o tempo médio de resolução, permitindo que os administradores solucionem problemas mesmo que a sessão tenha sido encerrada nas últimas 24 horas.

Para obter mais informações, consulte Métricas de Desempenho.

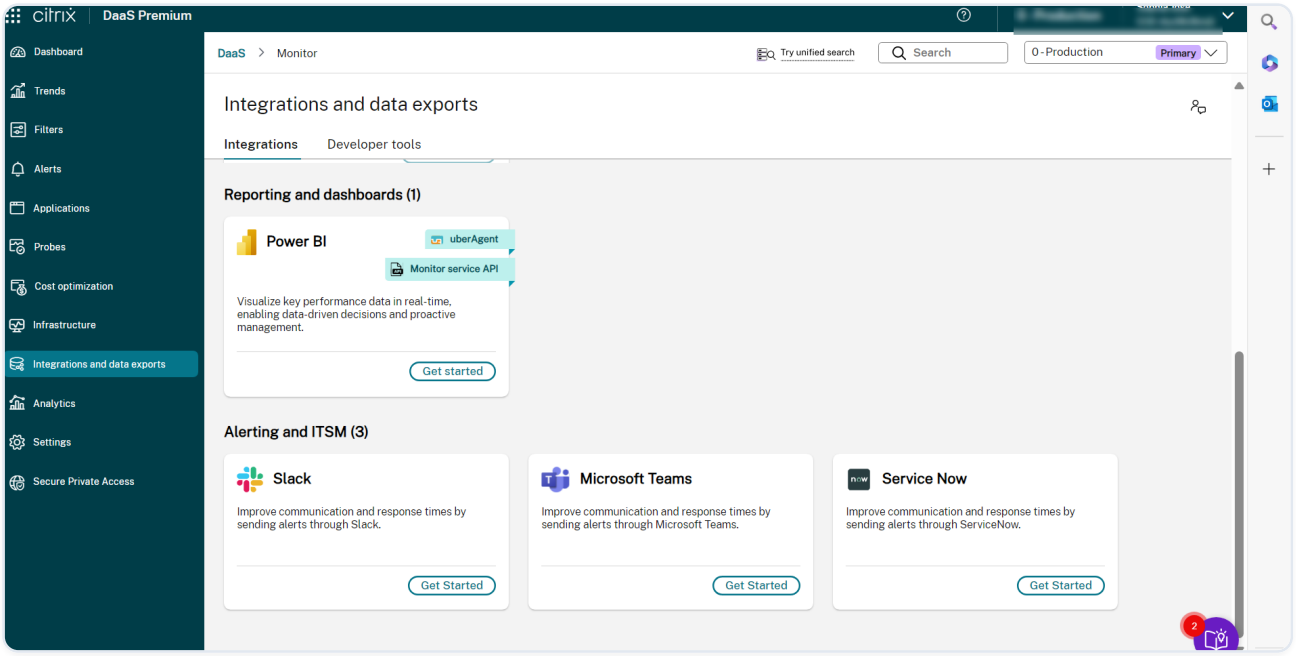
Integrações e exportações de dados. O Citrix Monitor agora oferece uma nova interface de usuário para integrações e exportações de dados. Este recurso ajuda a melhorar a conscientização sobre as várias interfaces e integrações de terceiros disponíveis no Citrix Monitor. A página de Integrações e Exportações de Dados recém-introduzida lista o seguinte:

- Integrações disponíveis
- Ferramentas de desenvolvedor suportadas

Esta página também descreve a configuração da API REST para exportação de dados e fornece links de referência para os guias e documentos para começar a usar as integrações e ferramentas de desenvolvedor.

Atualmente, o Citrix Monitor está integrado à observabilidade do Power BI. Você pode usar este recurso para exportar dados de desempenho e eventos do Citrix Monitor para o Power BI usando as APIs REST.

Clique em **Integrações e exportações de dados** no menu de navegação esquerdo. A página **Integrações e exportações de dados** é exibida.



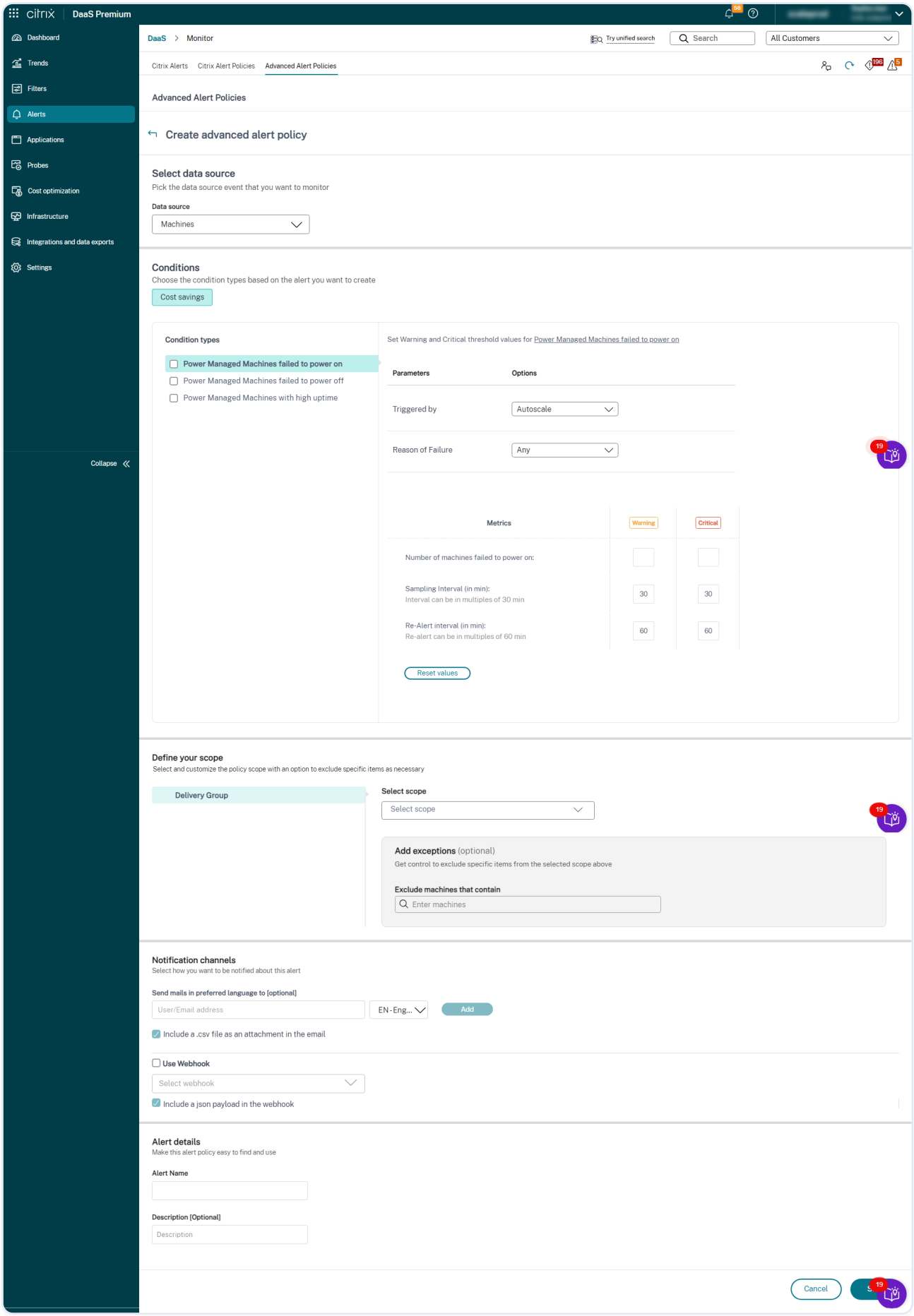
Para obter mais informações, consulte Integrações e exportações de dados.

Melhoria na triagem de problemas de carregamento de perfil de usuário. O Citrix Monitor agora oferece suporte à duração do carregamento do perfil e à coleta de métricas de contêiner do contêiner do Citrix Profile Management e do contêiner FSLogix. Essa melhoria auxilia o administrador a receber dados abrangentes de uso e desempenho do perfil em relatórios de

sessão do usuário. Com esses dados, você pode identificar e resolver problemas com maior eficiência. Para obter mais informações, consulte Carregamento de perfil.

Políticas de alerta avançadas. O recurso de Notificação e Alerta Proativo do Monitor foi aprimorado para incluir uma nova estrutura de alerta chamada **Políticas de Alerta Avançadas**. Com esse recurso, você pode criar alertas incluindo detalhes granulares para cada elemento ou condição, aumentando assim o controle sobre o escopo dos alertas. Atualmente, essas políticas incluem alertas para economia de custos e infraestrutura.

Esse recurso ajuda a reduzir alertas excessivos que podem levar à diminuição da capacidade de resposta ou eficácia na resolução de problemas importantes. Essa política ajuda a medir a eficácia das políticas de alerta e o engajamento dos administradores.



Para obter mais informações, consulte Políticas de alerta avançadas.

Aprimoramentos no conteúdo do alerta. O recurso de alerta do Monitor foi aprimorado para incluir um anexo CSV e um payload JSON. Com esse aprimoramento, você pode obter detalhes do alerta em um anexo CSV por e-mail ou como um payload JSON no caso de um webhook. Usando este anexo CSV e payload JSON, você pode receber conteúdo enriquecido em um nível detalhado, auxiliando na rápida identificação e resolução de problemas.

Atualmente, este aprimoramento está disponível apenas nos seguintes alertas:

- Tempo de atividade da máquina
- Ações de inicialização com falha
- Ações de desligamento com falha
- Máquinas não registradas (%)

Para obter mais informações, consulte Aprimoramentos no conteúdo do alerta.

Monitoramento de alerta de falha de sincronização de configuração do Local Host Cache. O Local Host Cache permite que as sessões do usuário continuem mesmo que os Cloud Connectors percam a conectividade com o Citrix Cloud. O cache usado pelo Local Host Cache é sincronizado regularmente com o banco de dados primário para garantir configurações atualizadas quando o modo Local Host Cache é ativado. Você pode obter mais informações sobre o Local Host Cache e o processo de sincronização de configuração em Local Host Cache. Se a sincronização da configuração falhar mais de três vezes consecutivas, o Citrix Monitor enviará um alerta de aviso ao administrador.

Uma política de alerta predefinida chamada **Local Host Cache - Falha na Sincronização da Configuração** foi introduzida no Citrix Monitor para notificar os administradores sobre falhas na sincronização da configuração. Você pode encontrar a política recém-introduzida em **Monitor** > **Alertas Citrix**. Para obter mais informações, consulte Monitoramento de alerta de falha de sincronização de configuração do Local Host Cache.

Alerta de ação de inicialização com falha e alerta de ação de desligamento com falha. O recurso de Notificação e Alerta Proativo do Monitor foi aprimorado para incluir dois novos alertas, **Ação de inicialização com falha** e **Ação de desligamento com falha**, com base no número de máquinas gerenciadas por energia que falharam ao ligar ou desligar em um grupo de entrega. A nova condição de alerta permite configurar limites de alerta como o número de máquinas gerenciadas por energia que falharam ao ligar ou desligar em um grupo de entrega.

Para mais informações, consulte Ação de ligar falha e Ação de desligar falha.

Monitoramento de infraestrutura (Pré-visualização). O Citrix Monitor agora oferece visibilidade sobre a saúde operacional dos componentes do Citrix Virtual Apps and Desktops. Este recurso ajuda você a identificar, solucionar e resolver facilmente problemas relacionados à sua infraestrutura. Atualmente, a saúde dos componentes Citrix Provisioning (PVS) e StoreFront é monitorada.

Para suportar este recurso, um novo executável do Windows chamado Citrix Infrastructure Monitor foi introduzido. Isso ajuda na coleta e transmissão de métricas de saúde relevantes dos servidores PVS ou StoreFront para o Monitor.

Este recurso ajuda você a obter conjuntos de dados de monitoramento críticos e alertas proativos em relação às métricas do sistema dos servidores PVS e StoreFront em um único console no Monitor. Os dados são coletados a cada cinco minutos dos componentes de monitoramento para garantir as informações mais recentes.

Este recurso visa aumentar a eficiência operacional, oferecendo monitoramento proativo, métricas detalhadas e alertas automatizados, garantindo que sua infraestrutura Citrix funcione de forma suave e eficiente. Para mais informações, consulte Monitoramento de infraestrutura [Pré-visualização].

Política de infraestrutura (Pré-visualização). Esta política é introduzida para criar alertas relacionados à saúde dos componentes suportados do Citrix Virtual Apps and Desktops.

Uma vez que a configuração de Monitoramento de infraestrutura esteja concluída, você pode usar os dados de saúde disponíveis no Monitor para configurar alertas para qualquer componente necessário. Os administradores podem definir condições, escopos e meios de notificação para receber alertas importantes por e-mail ou um payload JSON através de webhooks. Os alertas gerados também estão disponíveis na seção **Alertas Citrix** para análise e gerenciamento.

Como parte desta política, as quatro novas categorias a seguir são introduzidas:

- Acessibilidade
- Serviços dependentes
- Impacto
- Utilização de recursos

Você pode definir diferentes condições e modificar a severidade das categorias precedentes conforme necessário nas seções **Crítico** e **Aviso**. Você também pode agendar intervalos de re-alerta para esses alertas.

As condições dentro de cada categoria podem ser definidas com a severidade de Crítico e Aviso com base nas prioridades da sua organização. Você também pode agendar intervalos de re-alerta para esses alertas.

Para mais informações, consulte Políticas de infraestrutura (Pré-visualização).

Limite aumentado de réplicas por versão de imagem no Azure. O Azure aumentou a contagem máxima de réplicas para uma única versão de imagem de galeria para 100. Com o aumento do limite, agora você pode definir a propriedade `SharedImageGalleryReplicaMaximum` para um valor máximo de 100 ao criar um catálogo de máquinas MCS usando a imagem da Galeria de Computação do Azure. Para obter mais informações, consulte Configurar a Galeria de Computação do Azure.

Gerenciando imagens preparadas com o nó Imagens. Um nó **Imagens** agora está disponível na interface de Configuração Completa, que permite preparar uma imagem MCS (imagem preparada) a partir de uma única imagem de origem e implantá-la em vários catálogos de máquinas MCS. Este nó facilita o gerenciamento completo do ciclo de vida da imagem, permitindo que você crie definições de imagem, versões e catálogos.

As imagens preparadas usando este nó só podem ser usadas em ambientes Azure e VMware. Para obter informações detalhadas sobre o gerenciamento de imagens, consulte Gerenciamento de imagens (Visualização).

Alternativamente, você também pode criar catálogos com imagens preparadas usando o nó **Catálogos de Máquinas**. Para obter mais informações, consulte Criando catálogos de máquinas.

Relatório detalhado de configuração incorreta. Os alertas de configuração incorreta que são expostos no nó **Zonas** da interface de Configuração Completa fornecem informações gerais sobre uma configuração incorreta no local do recurso.

Com este aprimoramento, um novo cmdlet do PowerShell, `Get-ConfigMisconfigurationReport`, fornece um relatório detalhado de configurações incorretas na zona. Os detalhes adicionados incluem informações como qual Conector está configurado incorretamente, qual é a configuração incorreta atual e qual é a configuração recomendada. Consulte Solução de problemas para a documentação sobre configurações incorretas.

Introduzindo nomes de exibição de usuário e desktop no nó Pesquisar. Para melhorar a eficiência da sua solução de problemas, introduzimos duas novas colunas no nó Pesquisar:

- Coluna **Nome de Exibição do Usuário** na guia **Sessões**. Com esta coluna, você pode identificar rapidamente as sessões associadas a um usuário específico.

- Coluna **Nome de Exibição do Desktop** nas guias **Máquinas de SO de sessão única** e **Sessões**. Com esta coluna, você pode identificar rapidamente a máquina associada a um desktop específico.

Além disso, adicionamos filtros correspondentes para uma pesquisa eficiente. Para obter mais informações sobre essas duas colunas, consulte Ações e colunas da máquina e Ações e colunas da sessão.

Modificar nomes de exibição de desktop usando a Configuração Completa. Aprimoramos a página **Alocação de Máquina** para grupos de entrega estáticos de SO de sessão única, introduzindo uma nova coluna, **Nome de exibição**. Com esta adição, agora você pode modificar os nomes de exibição de desktop para máquinas atribuídas a usuários. Para obter mais informações, consulte Gerenciar atribuições de usuário.

Opções para solucionar problemas quando os dados de ICA RTT ou Duração de Logon da Sessão não são preenchidos. Anteriormente, quando o serviço EUEM ou o serviço UPM falhava ao ser executado, o motivo da falha na obtenção dos dados relacionados ao ICA RTT ou Duração de Logon da Sessão não era exibido. Com este novo recurso, você pode obter o motivo da falha e a solução correspondente para a falha. Para obter mais informações, consulte Solucionar problemas quando os dados de ICA RTT ou Duração de Logon da Sessão não são preenchidos.

Suporte para virtualização aninhada do Azure. Com este recurso, se você configurar a VM mestre com a virtualização aninhada habilitada, todas as VMs no catálogo de máquinas MCS criadas usando essa VM mestre terão a virtualização aninhada habilitada. Este recurso é aplicável a VMs persistentes e não persistentes. Você pode atualizar um catálogo de máquinas MCS existente e VMs existentes para ter virtualização aninhada por meio da atualização de imagem.

Atualmente, apenas os tamanhos de VM Dv3 e Ev3 suportam virtualização aninhada.

Para obter informações sobre virtualização aninhada, consulte o blog da Microsoft Virtualização Aninhada no Azure.

Suporte para herdar rótulos de uma origem de perfil de máquina para as VMs e discos no GCP. Com este recurso, as VMs e discos do catálogo de máquinas MCS (Disco de Identidade, Disco de Retorno de Cache de Gravação e disco do SO) agora podem herdar os rótulos de uma origem de perfil de máquina (instância de VM do GCP ou modelo de instância). Você pode usar os rótulos para distinguir instâncias pertencentes a diferentes equipes (por exemplo, **team:research** e **team:analytics**) e, além disso, usá-los para contabilidade de custos ou orçamento.

Para obter mais informações sobre rótulos, consulte o documento do GCP Organizar recursos usando rótulos.

Este recurso é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

Você pode criar um novo catálogo de máquinas MCS, atualizar um catálogo existente e atualizar VMs existentes para herdar os rótulos de uma origem de perfil de máquina.

Para obter informações sobre como criar um catálogo de máquinas MCS, consulte VMs e discos com rótulos herdados.

Suporte para herdar tags personalizadas do perfil da máquina para as VMs provisionadas. Agora você pode adicionar as tags personalizadas de uma VM SCVMM às VMs provisionadas do MCS junto com a tag padrão `CitrixProvisioningSchemeId`. Para adicionar as tags personalizadas às VMs provisionadas, você deve usar a VM SCVMM como um perfil de máquina ao criar ou atualizar um catálogo de máquinas MCS. Se você remover uma VM de um catálogo, apenas a `CitrixProvisioningSchemeId` será removida da tag. As tags personalizadas não são excluídas da VM. Este recurso se aplica a um novo catálogo de máquinas MCS e a novas VMs adicionadas a um catálogo existente. Para obter mais informações, consulte Criar um catálogo com um perfil de máquina.

Suporte para reserva de capacidade sob demanda no Azure. Com este recurso, você pode criar um catálogo de máquinas MCS de VMs do Azure com reserva de capacidade sob demanda usando um perfil de máquina (VM ou especificação de modelo). Este recurso é aplicável a catálogos de máquinas persistentes e não persistentes. Você pode atualizar um catálogo de máquinas existente e VMs existentes para ter ou remover a reserva de capacidade sob demanda.

Para obter mais informações sobre a reserva de capacidade sob demanda do Azure, consulte a documentação da Microsoft Reserva de Capacidade Sob Demanda. Para obter informações sobre como criar e atualizar um catálogo de máquinas MCS com reserva de capacidade sob demanda, consulte Criar um catálogo de VMs com reserva de capacidade sob demanda.

Suporte para colocar o disco WBC no mesmo local de armazenamento do disco do SO. Em ambientes de virtualização XenServer, VMware e SCVMM, o MCS agora coloca o disco de cache de gravação (WBC) no mesmo local de armazenamento do disco do SO se você configurar a lista de armazenamento de SO disponível da mesma forma que a lista de armazenamento temporário disponível ao criar uma conexão de host.

Esta implementação ajuda a reduzir a complexidade no gerenciamento dos discos do SO e WBC. Para criar uma conexão de host, consulte Criar uma conexão e recursos.

Melhoria na página de Economia de custos. A página de Economia de custos foi aprimorada com o seguinte:

- **Economia Estimada** - O gráfico de Economia Estimada agora inclui opções de filtro adicionais para visualizar dados dos últimos 7 e 30 dias. Ele também mostra a economia em relação aos preços específicos da conta do cliente.
- **Filtrar por Tags** - Exibe a tag das máquinas configuradas nas configurações de Autoscale em um WebStudio. Você também pode filtrar os dados com base nas máquinas marcadas. Neste caso, você obterá apenas o resumo das máquinas marcadas.
- **Duração média de logon** - Exibe o tempo médio para um usuário fazer logon durante o período de tempo selecionado.
- **Máquinas com gerenciamento de energia** - O gráfico de máquinas com gerenciamento de energia agora inclui o estado de hibernação da máquina, o que ajuda a analisar quantas máquinas estão em estado de hibernação.

Para obter mais informações, consulte a seção (/pt-br/citrix-daas/monitor/cost-optimization.html#cost-savings-preview).

Obtenha mensagens de aviso para falha de hibernação. Agora você pode obter mensagens de aviso usando um comando PowerShell `Get-ProvOperationEvent` em caso de falha de hibernação de VMs provisionadas por MCS e VMs existentes com capacidade de hibernação. Para obter mais informações, consulte (/pt-br/citrix-daas/install-configure/power-management/power-manage-azure-vms.html#get-warnings-messages-for-hibernation-failure).

Opção para atualizar as configurações de cache de write-back após a criação para catálogos do Machine Creation Service (MCS) nos hipervisores. Agora você tem a opção de atualizar o tamanho da memória e do cache de disco do cache de write-back, quando a Otimização de Armazenamento do Machine Creation Service (MCS) (MCSIO) está ativada, após a criação do catálogo para catálogos MCS nos hipervisores.

Para obter mais informações, consulte:

- Criar um catálogo de máquinas usando um perfil de máquina
- Criar um catálogo com um perfil de máquina
- Criar um catálogo de máquinas baseado em perfil de máquina usando PowerShell

Melhoria na guia Desempenho da Sessão. A seção **Topologia da Sessão** da guia **Desempenho da Sessão** foi aprimorada para incluir as seguintes métricas de endpoint que existem no aplicativo Citrix Workspace para Windows:

- Força do sinal WIFI
- Taxa de transferência de entrada e saída

- Tipo de interface de rede
- Velocidade do link

Essa melhoria ajuda a solucionar problemas relacionados a sessões rapidamente.

Diagnosticar sessões de usuário históricas . O Citrix Monitor agora exibe os detalhes das sessões em estado ativo, desconectado ou encerrado. Anteriormente, você só podia ver os detalhes das sessões ativas. Com este recurso, os administradores de helpdesk podem solucionar problemas com uma sessão que foi encerrada ou em estado de término. Os detalhes da sessão estão disponíveis para as últimas 24 horas e os últimos 2 dias. Você pode visualizar os seguintes detalhes de uma sessão encerrada ou terminada:

- Painel Detalhes da Máquina - Exibe os detalhes disponíveis da máquina onde a sessão selecionada foi iniciada.
- Painel de Detalhes da Sessão - Exibe os detalhes disponíveis da sessão selecionada.
- Duração do logon da sessão - Exibe as informações sobre a duração do logon para a sessão selecionada. Você pode visualizar o gráfico sobre o tempo gasto para corretagem, inicialização da máquina, conexão hdx, autenticação, GPOs, scripts de logon, carregamento de perfil em disco e sessão interativa.

Para obter mais informações, consulte Diagnosticar sessões de usuário históricas.

Alerta de tempo de atividade da máquina. O recurso de Notificação e Alerta Proativo do Monitor foi aprimorado para incluir um novo alerta, Alerta de tempo de atividade da máquina, baseado no tempo de atividade de uma máquina gerenciada por energia em um grupo de entrega. Para cada grupo de entrega, para o qual as máquinas excederam o limite, você receberá um anexo ou alerta de webhook apenas para esse grupo de entrega.

A nova condição de alerta permite configurar limites de alerta como o número de horas por dia, horas por semana ou horas por mês em que uma máquina é ligada em um grupo de entrega.

Para obter mais informações, consulte Alerta de tempo de atividade da máquina.

Nome do desktop publicado. O Citrix Monitor agora exibe o nome do desktop publicado na interface do usuário. Este novo campo permite diferenciar entre grupos de usuários dentro do mesmo grupo de entrega. Você também pode gerar relatórios personalizados para esses grupos de usuários. Este novo campo é adicionado a **Filtros**, **Relatórios Personalizados** ou à seção **Detalhes da Máquina** da interface do usuário do Citrix Monitor.

Dimensionamento de infraestrutura. A página **Dimensionamento de Infraestrutura** ajuda você a analisar os aspectos de provisionamento e dimensionamento do seu grupo de entrega com base na utilização dos recursos. Com base nesta análise, você pode otimizar o provisionamento e o dimensionamento da máquina para corresponder ao padrão de utilização. Você pode otimizar o custo da sua infraestrutura reduzindo os gastos com recursos não utilizados. Você também pode optar por máquinas com especificações de CPU e memória mais baixas se a utilização dos recursos for consistentemente menor do que o provisionado. Você pode otimizar o desempenho optando por máquinas com especificações de CPU e memória mais altas se a utilização dos recursos for consistentemente maior e houver evidências de que isso afeta a experiência da sessão, como as métricas de *Logon e ICARTT*.

Você pode filtrar o dimensionamento da infraestrutura usando o seguinte:

- Grupo de Entrega - Você pode filtrar por grupos de entrega de SO de sessão única ou SO de múltiplas sessões
- Tags - Tags são os nomes de tags aplicados à máquina. Assim, você pode filtrar máquinas com as mesmas tags. Você pode selecionar várias tags, até cinco tags. Ao selecionar várias tags, você pode filtrar todas as máquinas que possuem pelo menos uma das tags de máquina selecionadas aplicadas.
- Período de tempo - Você pode filtrar os dados para as últimas 24 horas, 7 dias e 30 dias.

A página de dimensionamento da infraestrutura oferece:

- Visão detalhada dos detalhes de utilização
- Resumo da utilização dos recursos
- Tendências na utilização de recursos

Clique na guia **Otimização de Custos** no menu esquerdo da página inicial. Em seguida, clique na guia **Dimensionamento de infraestrutura** para acessar a página **Dimensionamento de infraestrutura**.

Você também pode clicar no link **Dimensionar este grupo de entrega** na seção **Detalhes da infraestrutura** na guia **Otimização de Custos** > **Economia de custos** para acessar a página **Dimensionamento de infraestrutura**.

Para obter mais informações, consulte Dimensionamento de infraestrutura.

Painel de atividades do Cache de Host Local. O novo painel do Cache de Host Local, na **guia Tendências**, fornece informações detalhadas sobre as sessões de usuário e as máquinas disponíveis durante uma interrupção em qualquer local de recurso ou Zona. Os administradores

podem usar os detalhes sobre o número de registros de máquinas, sessões reconectadas e novas sessões intermediadas para avaliar e auditar as atividades enquanto estiverem no modo Cache de Host Local. Os dados selecionados por padrão são para as últimas 24 horas e para todos os conectores de zona e nuvem, com a capacidade de filtrar por período de tempo, zona e conector de nuvem. Os dados do Cache de Host Local estão disponíveis para as últimas 2 horas, 24 horas, 7 dias, 1 mês e até 90 dias. Para obter mais informações, consulte Tendências disponíveis.

Especifique chaves CMEK globais e regionais de todos os projetos. Em ambientes Google Cloud, anteriormente, você só podia usar a chave de criptografia gerenciada pelo cliente (CMEK) do mesmo projeto GCP e da mesma região em que a conexão de hospedagem foi criada.

Com este recurso, agora você pode navegar e usar CMEK global ou regional de todos os projetos acessíveis à conta de serviço. Este recurso aumenta a flexibilidade para gerenciar chaves de criptografia. Este recurso requer permissão extra para as duas contas de serviço a seguir:

- A conta de serviço do projeto atual com a qual a conexão de hospedagem é criada.
- O Agente de Serviço do Compute Engine do projeto atual.

Para obter mais informações, consulte Especificar chaves CMEK globais e regionais.

Workspaces Desacoplados, permitem atribuição de userGroup. Workspaces Desacoplados agora permitem um gerenciamento mais flexível e independente de usuários e seus workspaces associados. Isso significa simplesmente que você pode criar implantações sem associar nenhum usuário a elas e, em vez disso, atribuir os usuários a uma implantação posteriormente. Para obter mais informações, consulte Criar uma implantação.

Suporte para importar o tipo de imagens do Workspace. Agora você pode importar o tipo de imagens do Workspace para criar uma experiência de desktop para os usuários. Para obter mais informações, consulte Importar uma imagem.

Função de exportação estendida a todos os nós na Configuração Completa. Agora você pode exportar registros da exibição principal de qualquer nó na Configuração Completa para um arquivo CSV. Observe o seguinte:

- O ícone **Exportar** é desativado enquanto os dados estão sendo carregados, exceto para os nós **Pesquisar** e **Aplicativos**.
- Para nós com a função **Colunas a Exibir**, os dados exportados incluem apenas as colunas selecionadas.

Suporte para adicionar notas para o modo de manutenção. Agora você pode adicionar notas ao colocar uma máquina, grupo de entrega ou conexão em modo de manutenção. Essas notas ficam visíveis no campo **Motivo da manutenção** do painel Detalhes, ajudando você e outros administradores a entender o motivo da manutenção.

Cache de dados para os nós Zonas e Políticas. Introduzimos o cache de dados para os nós **Zonas** e **Políticas**. Essa melhoria reduz significativamente o tempo de carregamento da página quando você navegar para um nó, melhorando a experiência geral do usuário.

Opção para atualizar a configuração do cache de write-back após a criação para catálogos do Machine Creation Service (MCS) no Google Cloud Platform.

Agora você tem a opção de atualizar o tamanho da memória e do cache de disco do cache de write-back, quando a Otimização de Armazenamento do Machine Creation Service (MCS) (MCSIO) está habilitada, após a criação do catálogo para catálogos MCS no Google Cloud Platform.

Para obter mais informações, consulte Criar um catálogo de máquinas usando a interface de Configuração Completa.

Opção para gerenciar manualmente a função do principal de serviço para o gerenciamento de dispositivos ingressados no Azure AD.

Aprimoramos a opção **Habilitar gerenciamento de dispositivos ingressados no Azure AD** para maior flexibilidade. Anteriormente, você precisava fazer login no Azure e permitir que a Citrix atribuísse a função de **Administrador de Dispositivos na Nuvem** ao principal de serviço da conexão em seu nome. Esse design funcionava apenas quando sua conta do Azure tinha permissão para conceder essa função.

Com essa melhoria, se sua conta do Azure não tiver a permissão necessária, agora você pode escolher Não fazer login no Azure ao habilitar o gerenciamento de dispositivos ingressados no Azure AD. Isso permite que você atribua manualmente a função ao principal de serviço da conexão no portal do Azure.

Para obter mais informações, consulte Habilitar gerenciamento de dispositivos ingressados no Azure AD.

Instalar o agente FlexApp One. A Liquidware possui um pacote chamado FlexApp One. O agente FlexApp One agrupa os aplicativos de software junto com suas configurações e dependências para fácil distribuição e implantação em um arquivo compartilhável.

Para oferecer suporte à descoberta e publicação de pacotes Liquidware FlexApp One, instale o agente FlexApp One em qualquer VDA usado para descoberta ou inicialização de pacotes. Para obter mais informações, consulte Instalar o Agente FlexApp One.

Junho de 2024

Novos recursos e aprimoramentos

Configuração Completa: Suporte para provisionamento de VMs VMWare usando perfil de máquina. Ao provisionar VMs VMWare usando o Machine Creation Services (MCS), agora você pode selecionar um modelo existente como perfil de máquina, permitindo que as VMs dentro do catálogo herdem as configurações do modelo selecionado.

As configurações herdadas incluem:

- Tags colocadas no modelo
- Atributos personalizados
- Políticas de armazenamento vSAN
- Versão do hardware virtual
- vTPM (TPM Virtual) do vSphere
- Contagem de CPU e núcleos por soquete
- Contagem de NIC

Crie grupos de entrega exclusivamente para VMs com capacidade de suspensão usando a Configuração Completa. Introduzimos uma nova opção em **Configuração Completa > Criar Grupo de Entrega**, **Tornar a capacidade de suspensão obrigatória para este grupo de entrega**. Esta opção permite criar grupos de entrega que contêm apenas VMs com capacidade de suspensão, facilitando o gerenciamento de energia da sua máquina no nível do grupo de entrega. Observe que este recurso se aplica apenas a VMs de SO de sessão única.

Para obter mais informações, consulte Criar grupos de entrega.

Painel de Métricas de Desempenho aprimorado. O painel **Métricas de Desempenho** possui uma visualização aprimorada das métricas de dados históricos. Ao clicar na guia **Desempenho da Sessão**, juntamente com os dados em tempo real, você pode visualizar os dados dos últimos 15 minutos sem esperar pelo tempo de carregamento da página. Este aprimoramento ajuda a reduzir o tempo médio de resolução, permitindo que os administradores correlacionem várias métricas de

desempenho de componentes em uma única visualização. Para obter mais informações, consulte Métricas de Desempenho.

Visualização de Logon de Sessão aprimorada. - A nova opção **Inicialização da Máquina** com as seguintes subseções na guia **Logon de Sessão** na página **Filtros** -> **Detalhes do Usuário** fornece um detalhamento do tempo necessário para iniciar uma máquina virtual durante diferentes fases:

- **Ligar** - Exibe o tempo necessário para ligar uma máquina virtual
- **Inicialização e registro** - Exibe o tempo necessário para inicializar e registrar uma máquina virtual

O botão recolhível recém-introduzido na página **Logon de Sessão** ajuda a recolher ou expandir as opções em **Inicialização da Máquina** e **Sessão Interativa**.

Juntamente com as opções padrão da tabela **Fases de Duração do Logon**, que são **Fase de Logon da Sessão** e **Duração**, você também pode escolher as seguintes colunas na página **Logon de Sessão**:

- Hora de início
- Hora de término
- Média de 7 dias do Grupo de Entrega (seg)
- Média de 7 dias do Usuário (seg)

Você também pode exportar os dados anteriores para um arquivo .CSV.

As colunas recém-adicionadas **Ligar** e **Inicialização e registro** podem ser adicionadas à tabela **Duração do Logon por Sessão do Usuário** em **Tendências** -> **Desempenho do Logon** > **Escolher Colunas**. Você também pode exportar os relatórios na tela **Desempenho do Logon**.

Este aprimoramento ajuda a entender e solucionar facilmente problemas relacionados à duração do logon. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Alerta de máquinas não registradas. O recurso de Notificação e Alerta Proativo do Monitor foi aprimorado para incluir um novo alerta, **Máquinas não registradas (em %)**, com base na porcentagem de máquinas não registradas em um grupo de entrega. A nova condição de alerta permite configurar valores de limite de aviso e crítico como uma porcentagem de máquinas não registradas em um grupo de entrega. Para obter mais informações, consulte a seção Máquinas não registradas (em %) no artigo Alertas.

Conexões de diretório compartilhadas ou dedicadas. Agora você pode criar conexões de diretório usando tenências dedicadas ou compartilhadas. Se a tenência dedicada for selecionada ao adicionar uma conexão de diretório, os espaços de trabalho criados serão para desktops de sessão única. Se a tenência compartilhada for selecionada ao adicionar uma conexão de diretório, os espaços de trabalho criados serão compartilhados. Para obter mais informações, consulte:
Conexões de diretório compartilhadas ou dedicadas. Agora você pode criar conexões de diretório usando tenências dedicadas ou compartilhadas:

- Se você selecionar a tenência dedicada ao adicionar uma conexão de diretório, os espaços de trabalho criados serão para desktops de sessão única.
- Se você selecionar a tenência compartilhada ao adicionar uma conexão de diretório, os espaços de trabalho criados serão compartilhados. Para obter mais informações, consulte:
  - Criar uma conexão de diretório
  - Importar uma imagem
  - Criar uma implantação

Proteção de Aplicativos Contextual. Com este recurso, os administradores podem aplicar o controle **App Protection Anti-Screen Capture** e **Anti-keylogging** em dispositivos e usuários de forma contextual, em vez de ter os controles sempre ativados ou sempre desativados. Esta implementação ajuda a aplicar o **App Protection Anti-Screen Capture** e o **Anti-keylogging** apenas quando necessário. Para obter mais informações, consulte Etapa 7. Proteção de aplicativos e Gerenciar proteção de aplicativos.

Configurações de exibição padrão aprimoradas para catálogos de máquinas, grupos de entrega e aplicativos. Introduzimos novas opções de exibição padrão para Catálogos de Máquinas, Grupos de Entrega e Aplicativos, oferecendo maior flexibilidade e personalização:

- **Seleção de exibição padrão.** Anteriormente, esses nós tinham como padrão uma exibição de pasta, que era adequada para organizações que usavam estruturas de gerenciamento baseadas em pastas. Com a introdução de um ícone de **Pasta** na barra de ações, agora você pode alternar entre a exibição de pasta e a exibição de lista como sua exibição padrão preferida.
- **Exibição de pasta aprimorada.** A alternância **Exibir tudo** agora mantém sua última seleção quando você faz login novamente. Se desativada anteriormente, ela permanecerá desativada, com a pasta raiz selecionada e as subpastas de primeiro nível expandidas.

Cache de dados para o nó StoreFront. Introduzimos o cache de dados para o nó **StoreFront**. Esse aprimoramento reduz significativamente o tempo de carregamento da página quando você navegar para o nó **StoreFront**, melhorando a experiência geral do usuário.

Pesquisa de nome de usuário aprimorada na criação de catálogo de máquinas. Aprimoramos a funcionalidade de pesquisa de administradores por nomes de usuário durante a criação de catálogo de máquinas. Os principais aprimoramentos na página **Configuração do Catálogo de Máquinas > Inserir Credenciais** incluem:

- **Especificação de domínio:** Uma nova opção, **Domínio**, agora está disponível nessa página, permitindo que você restrinja a pesquisa inserindo o nome do domínio ou SID.
- **Otimização da pesquisa SamName:** As pesquisas usando SamName agora estão restritas ao domínio especificado.

Esses aprimoramentos tornam as pesquisas de usuário mais rápidas e eficientes.

Atualizações simplificadas de sub-redes para catálogos de máquinas. Anteriormente, para alterar as configurações de sub-rede de um catálogo de máquinas, era necessário excluí-lo e recriá-lo. Com esse recurso, agora você pode obter a mesma funcionalidade editando o catálogo. Observe que apenas as novas máquinas virtuais criadas no catálogo estarão nas sub-redes recém-associadas. Esse aprimoramento reduz a necessidade de exclusão de catálogo e tarefas associadas. Para obter mais informações, consulte Editar um catálogo.

Suporte para criação de grupos de recursos durante a criação de catálogo do Azure (para PVS). Anteriormente, ao criar catálogos do Azure usando a Configuração Completa, era necessário criar os grupos de recursos usando comandos do PowerShell. Com esse recurso, agora você pode criar um grupo de recursos de forma contínua como parte da criação do catálogo no Web Studio. Esse aprimoramento simplifica o fluxo de trabalho geral de criação. Para obter mais informações, consulte Criar um catálogo do Citrix Provisioning usando a interface de configuração completa.

Maio de 2024

Novos recursos e aprimoramentos

HDX Seguro (Pré-visualização). Agora você pode usar esse recurso para evitar que qualquer elemento de rede no caminho do tráfego possa inspecionar o tráfego HDX. Para obter mais informações, consulte HDX Seguro.

Suporte à hibernação de GPU do Azure (Pré-visualização). Agora você tem a opção de oferecer suporte à hibernação para SKUs de máquina do Azure que suportam GPU. Para obter mais informações sobre os tamanhos de VM suportados, consulte a documentação da Microsoft.

Suporte a catálogos do Citrix Provisioning para junção híbrida do Azure AD estendido para Configuração Completa. Ao criar um catálogo do Citrix Provisioning, o tipo de identidade **Ingressado no Azure Active Directory Híbrido** agora está disponível na página **Configuração do Catálogo de Máquinas > Identidades da Máquina**. Com essa nova opção, você pode criar máquinas ingressadas no Azure AD híbrido por meio do Citrix Provisioning. Para obter mais informações, consulte este artigo do Citrix Provisioning.

Aprimoramentos na ajuda contextual da Configuração Completa. Redesenhamos o painel de ajuda para fornecer uma experiência mais informativa, oferecendo informações direcionadas para cada nó dentro da Configuração Completa. Ao clicar no ícone de Ajuda em qualquer nó, agora você pode acessar um conjunto abrangente de recursos destinados a fornecer uma experiência de aprendizado completa, ajudando você a entender melhor os recursos relacionados:

- Acesse documentos-chave especificamente relacionados ao nó selecionado.
- Mantenha-se informado sobre as atualizações de serviço, incluindo Roteiro da Citrix, Problemas conhecidos, Limites, Requisitos do sistema e Recursos novos.
- Acesse recursos expandidos como Blogs da Citrix, Comunidade Citrix, Recurso Citrix Explicado, Documentação do Produto Citrix, Suporte Citrix e Documentação do Desenvolvedor.

Registro de configuração aprimorado: rastreamento de alterações de associação para grupos de entrega. Com este aprimoramento, o registro de configuração agora captura e exibe IDs de usuários e grupos adicionados ou removidos de grupos de entrega. Para visualizar os logs de configuração, vá para **Configuração Completa > Registro > Eventos**.

Personalize a ordem das guias no nó Pesquisar. Agora você pode personalizar a ordem das guias no nó **Pesquisar** de acordo com seus padrões de uso, aprimorando a experiência de navegação. Para fazer isso, clique no ícone de três pontos ao lado das guias, arraste as guias para a ordem preferida e, em seguida, clique em **Aplicar**.

Cache de dados para o nó Catálogos de Máquinas. Introduzimos o cache de dados para o nó **Catálogos de Máquinas** do Citrix DaaS. Este aprimoramento reduz significativamente os tempos de carregamento da página quando você navegar para o nó **Catálogos de Máquinas**, melhorando a experiência geral do usuário.

Suporte para criação de catálogos do Citrix Provisioning usando comandos MCS PowerShell no VMware. Agora você pode criar catálogos do Citrix Provisioning usando comandos MCS PowerShell no VMware.

Esta implementação oferece as seguintes vantagens:

- Uma única API unificada para gerenciar catálogos MCS e Citrix Provisioning.
- Ter novos recursos para catálogos do Citrix Provisioning, como solução de gerenciamento de identidade, provisionamento sob demanda e assim por diante.

Para obter mais informações, consulte Criar catálogos do Citrix Provisioning no Citrix Studio.

Detecção e Mitigação de Falhas no Serviço de Atualização de VDA Durante o processo de atualização de VDA (Pré-visualização). Nosso serviço agora incorpora mecanismos avançados de detecção. Se forem detectados quaisquer problemas que possam levar à falha da IPU do VDA, tornando o VDA inutilizável, o serviço tomará medidas proativas. Ele deixará de atualizar máquinas adicionais e sairá graciosamente do fluxo de trabalho atual. Essa abordagem proativa visa minimizar o impacto e garantir uma experiência tranquila, mesmo em caso de desafios inesperados, reduzindo o raio de impacto potencial de quaisquer problemas encontrados. Para obter mais informações, consulte Detecção e Mitigação de Falhas no Serviço de Atualização de VDA

Suporte a atualizações de VDA a partir de um compartilhamento de arquivos local ao qual os VDAs têm acesso (Pré-visualização). Com o Controle de Acesso Aprimorado do Instalador de VDA, agora você pode ter maior flexibilidade e controle sobre quais VDAs podem se conectar e recuperar os MSIs de download necessários sem se preocupar em conceder acesso à rede para que os VDAs busquem atualizações do Citrix Managed Azure CDN. Isso permite que você aplique regras de rede mais rigorosas, garantindo acesso contínuo a atualizações essenciais. Para obter mais informações, consulte Suporte a atualizações de VDA a partir de um compartilhamento de arquivos local ao qual os VDAs têm acesso

Suporte de Configuração Completa para entrega de aplicativos empacotados para desktops estáticos de sessão única e PCs de escritório. Com este aprimoramento, agora você pode entregar aplicativos empacotados para todos os tipos de desktops usando a Configuração Completa. Os benefícios da entrega de aplicativos empacotados para desktops *estáticos de sessão única* incluem:

- Os aplicativos estão disponíveis no VDA no momento do login e não são preparados sob demanda através do Workspace ou StoreFront.
- Tempo de inicialização aprimorado ao acessar os aplicativos empacotados.

- Facilita a manutenção dos aplicativos empacotados de forma independente, separadamente da imagem base do VDA.

Para entregar aplicativos empacotados a desktops, adicione esses aplicativos aos grupos de entrega usando estas formas:

- Adicione aplicativos durante a criação do grupo de entrega.
- Adicione aplicativos a um grupo de entrega existente usando uma destas entradas: **Delivery Groups > Add Applications > Applications**, **Applications > Properties > Groups**, ou **App Packages > Packages > Add Delivery Groups**.

Para obter mais informações, consulte Criar grupos de entrega, Gerenciar grupos de entrega e Adicionar aplicativos a grupos de entrega.

Suporte à Configuração Completa para entrega de aplicativos empacotados no formato FlexApp. Em **Full Configuration > App Packages**, agora você pode carregar aplicativos empacotados FlexApp para o Citrix Cloud e entregá-los aos seus usuários. Para obter mais informações, consulte Pacotes de aplicativos.

Paginação OData. O Monitor aprimora o limite da paginação OData. Todos os endpoints OData v4 retornam um máximo de 1000 registros por página com um link para os próximos 1000 registros na resposta. Como cada página retorna grandes conjuntos de dados, você pode obter a mesma quantidade de dados totais com menos consultas OData. Assim, este recurso reduz o tempo para obter os dados totais e, consequentemente, melhora a experiência do usuário. Para obter mais informações, consulte a documentação Acessando dados do serviço Monitor usando o endpoint OData v4 no Citrix Cloud.

Suporte para criar e gerenciar VMs confidenciais do Azure usando a Configuração Completa. As VMs confidenciais do Azure fornecem um limite forte e imposto por hardware para ajudar a atender às suas necessidades de segurança. Com a interface de usuário da Configuração Completa, agora você pode criar e gerenciar VMs confidenciais no Azure. Para obter mais informações, consulte VMs confidenciais do Azure (Visualização).

Suporte para exibir IPs de cliente em logs de configuração. Em **Full Configuration > Logging > Events**, agora você pode visualizar detalhes de endereço IP nos logs, facilitando o rastreamento das origens das ações. Para mostrar a coluna de endereço IP na visualização principal, clique no ícone **Columns to Display** no canto superior direito dos logs e, em seguida, selecione **Client IP**. Para obter mais informações, consulte Visualizar conteúdo do log de configuração.

Suporte para capturar propriedades adicionais usando a origem do perfil da máquina na AWS. Em ambientes AWS, com este aprimoramento, agora você pode criar ou atualizar um catálogo baseado em perfil de máquina para incluir o seguinte:

- Capturar opções de CPU, tipo de locação e capacidade de hibernação da origem do perfil da máquina ao criar um catálogo de máquinas MCS.
- Alterar o tipo de locação da origem do perfil da máquina ao editar um catálogo de máquinas MCS. Esta funcionalidade é aplicável apenas às novas VMs adicionadas ao catálogo.
- Alterar a capacidade de hibernação da origem do perfil da máquina ao editar um catálogo de máquinas MCS. Esta funcionalidade é aplicável apenas às novas VMs adicionadas ao catálogo.

A origem do perfil da máquina pode ser uma VM ou uma versão de modelo de inicialização. Este recurso é aplicável a catálogos persistentes e não persistentes.

Para obter mais informações, consulte Criar um catálogo de máquinas baseado em perfil de máquina usando o PowerShell.

Reparar as informações de identidade de contas de computador ativas no AWS. Em ambientes AWS, agora você pode redefinir as informações de identidade de contas de computador ativas que apresentam problemas relacionados à identidade. Você pode optar por redefinir apenas a senha da máquina e as chaves de confiança, ou redefinir toda a configuração do disco de identidade. Essa implementação é aplicável a catálogos de máquinas MCS persistentes e não persistentes. Atualmente, o recurso é suportado apenas para ambientes de virtualização AWS, Azure e VMware. Para obter mais informações, consulte Reparar as informações de identidade de contas de computador ativas.

Suporte para criptografia do disco de ID de VMs de catálogo de máquinas MCS no AWS. Anteriormente, em ambientes AWS, o MCS permitia a criptografia apenas do disco do SO das VMs provisionadas. Com esse recurso, agora você pode criptografar o disco de ID além do disco do SO. Essa funcionalidade permite que você use chaves AWS KMS (chave gerenciada pelo cliente e chave gerenciada pela AWS) para realizar operações criptográficas nos discos anexados a uma VM.

Para criptografia de discos de SO e ID, configure um dos seguintes:

- Use uma imagem mestre criptografada (por exemplo, uma AMI criada a partir de uma instância ou snapshot que contém um volume raiz criptografado com chave KMS)
- Use uma origem de perfil de máquina (VM ou modelo de inicialização) que contenha um volume raiz criptografado.

Para obter mais informações, consulte Criptografar discos de SO e ID.

Configurar grupos de segurança por interface de rede no AWS. Ao editar uma conexão de host para ambientes AWS, agora você pode configurar o número máximo de grupos de segurança permitidos por interface de rede elástica (ENI) usando um comando PowerShell. Portanto, se você aumentar sua cota de grupos de segurança por interface de rede, poderá configurar o mesmo valor para a conexão de hospedagem. Para obter informações sobre a configuração, consulte Configurar grupos de segurança por interface de rede.

Otimização de custos . A página **Otimização de Custos** fornece uma representação visual das economias de infraestrutura acumuladas durante um período selecionado e prevê as economias esperadas para os dias restantes. Ao analisar o uso da máquina e as sessões, esta página ajuda você a identificar as economias alcançadas e as oportunidades de redução de custos. Esta página oferece:

- Visão sobre a otimização dos custos de infraestrutura
- O valor economizado
- Informações sobre uma variedade de cenários que podem resultar em custos projetados excedidos
- Oportunidades potenciais para identificação e planejamento estratégico para realizar economias de custos de infraestrutura

A **página Otimização de Custos** inclui **Economias estimadas** e **Relatório de economias do Autoscale**.

A **Economia estimada** ajuda a avaliar a utilização eficiente dos recursos de infraestrutura. A economia de custos é exibida em dólares americanos ou como uma porcentagem do custo incorrido. Você pode visualizar os resultados dos últimos 3, 6 e 12 meses. O gráfico **Economia estimada** exibe o seguinte:

- Economia estimada - Exibe o valor da economia alcançada na infraestrutura para a duração selecionada
- Máquinas com gerenciamento de energia - Exibe o número total de máquinas com gerenciamento de energia.
- Economia projetada - Exibe quanta economia de infraestrutura pode ser feita para a duração restante

O **Relatório de economia do Autoscale** exibe informações sobre o grupo de entrega para o qual o Autoscale está configurado e habilitado. Este relatório é aplicável apenas para máquinas com gerenciamento de energia. Para obter mais informações, consulte a página Otimização de Custos.

Inspecionar máquinas com ações de energia recentes. Agora você pode inspecionar máquinas com o status das ações de energia bem-sucedidas e falhas. Este recurso ajuda você a analisar o seguinte:

- Falha ao ligar que causa problemas ao usuário
- Falha ao desligar que aumenta o custo

> **Observação:**
>
> Os dados estão disponíveis apenas para a máquina com gerenciamento de energia. Os dados não estão disponíveis para as ações de energia realizadas antes que o recurso fosse suportado.

> Você pode visualizar o status da ação de energia das máquinas das seguintes maneiras:

- Na guia **Filtros** -> **Máquinas**. Nesse caso, por padrão, as colunas **Hora da Ação de Energia** e **Resultado da Ação de Energia** ficam visíveis. Você também pode selecionar as colunas que deseja tornar visíveis.
- Na guia **Otimização de Custos**. Nesse caso, o filtro padrão **Ação de Energia Acionada Por** é definido como *Autoscale* e o **Resultado da Ação de Energia** é definido como *Falha*.

Com este recurso, você pode visualizar os detalhes dos controles de ação de energia. Por exemplo, você pode ver quem acionou a ação, qual ação alterou o estado de energia, o motivo da falha e a hora em que a ação foi concluída. Você também pode exportar esses detalhes.

Para obter mais informações, consulte Inspecionar máquinas com ações de energia recentes.

Abril de 2024

Recursos novos e aprimorados

Suporte para uma versão mais recente do Microsoft Teams. O Citrix Monitor agora oferece suporte ao Microsoft Teams versão 2.1 ou anterior.

Alterar a criptografia de disco no Azure. Com este recurso, agora você pode alterar a criptografia de disco em ambientes de virtualização do Azure. Você pode fazer o seguinte:

- Crie um catálogo de máquinas MCS com um conjunto de criptografia de disco (DES) diferente do DES da imagem mestre.
- Altere o tipo de criptografia de disco de uma chave DES para outra chave DES de um catálogo de máquinas MCS existente e VMs existentes.
- Atualize um catálogo de máquinas MCS e uma VM que não estavam habilitados para CMEK anteriormente para ter criptografia de chave de criptografia gerenciada pelo cliente (CMEK) (DES), criptografia de disco no host ou criptografia dupla.
- Atualize um catálogo de máquinas MCS e uma VM existentes para não serem criptografados, se foram criptografados anteriormente.
- Habilite a criptografia de disco com ponto de extremidade privado (um catálogo de máquinas MCS que usou uma conexão de host habilitada com `ProxyHypervisorTrafficThroughConnector`).

Para obter mais informações, consulte Alterar a criptografia de disco.

Suporte para modificação das configurações do arquivo de paginação. Com este recurso, você pode modificar as configurações do arquivo de paginação das VMs recém-adicionadas a um catálogo existente sem atualizar a imagem mestre. Atualmente, este recurso é aplicável apenas a ambientes Azure.

Para modificar as configurações do arquivo de paginação, você precisa da versão 2311 do VDA ou posterior. Você pode modificar as configurações do arquivo de paginação usando os comandos do PowerShell. Para obter mais informações sobre como modificar as configurações do arquivo de paginação, consulte Modificar configurações do arquivo de paginação.

Verificar várias NICs no VMware. Em ambientes VMware, introduzimos várias verificações pré-voo quando a unidade de hospedagem e o modelo de perfil de máquina têm várias redes, e o parâmetro `-NetworkMapping` é usado nos comandos `New-ProvScheme` e `Set-ProvScheme`. Para obter mais informações sobre a lista de verificação pré-voo para várias NICs, consulte Verificar várias NICs.

Suporte para criação de VMs do Windows 11 no GCP. Agora você pode criar VMs do Windows 11 no GCP. Se você instalar o Windows 11 na imagem mestre, deverá habilitar o vTPM durante o processo de criação da imagem mestre. Além disso, você deve habilitar o vTPM na origem do perfil da máquina (VM ou modelo de instância).

Este recurso é aplicável a:

- Catálogos de máquinas MCS persistentes e não persistentes.
- Apenas grupo de nós de locatário único.

Para obter informações sobre como criar VMs do Windows 11 no nó de locatário único, consulte Criar VMs do Windows 11 no nó de locatário único.

Suporte à lista de permissões de canal virtual para variáveis de ambiente. Agora você pode usar variáveis de ambiente do sistema no caminho dos processos confiáveis. Para obter mais informações, consulte Usando variáveis de ambiente do sistema.

Recursos obsoletos na Configuração Completa. Os seguintes recursos e configurações foram preteridos na Configuração Completa:

- Ambientes Azure:

  O provisionamento de VMs usando uma imagem mestre de uma região diferente foi preterido. Recomendamos usar a Galeria de Computação do Azure para replicar a imagem mestre para a região onde as VMs serão criadas.

- Ambientes AWS:

  A opção **Aplicar propriedades de modelo de máquina a máquinas virtuais**, na página **Configuração do Catálogo de Máquinas > Modelo de Máquina**, foi preterida. Recomendamos usar perfis de máquina para especificar as propriedades da máquina para VMs.

- Todos os ambientes de hipervisor e serviço de nuvem:

  A configuração do cache de write-back com apenas um cache de disco e sem cache de memória foi preterida. Recomendamos definir o tamanho do cache de memória para um valor maior que zero.

Experiência aprimorada de interrupção de serviço na Configuração Completa. Para aprimorar sua experiência durante interrupções de serviço, melhoramos o conteúdo da notificação na página Configuração Completa. Com este aprimoramento, agora você pode obter uma compreensão mais clara das interrupções de serviço, como as causas, as etapas para habilitar o serviço e os tempos estimados de habilitação. Este aprimoramento abrange as seguintes interrupções de serviço:

- Solicitações de habilitação de serviço para o primeiro uso
- Pausas de serviço causadas por inatividade prolongada

- Interrupções de serviço causadas pela indisponibilidade do DaaS

Cache de dados para o nó de Hospedagem. Introduzimos o cache de dados para o nó **Hospedagem** do Citrix DaaS. Essa melhoria reduz significativamente os tempos de carregamento da página quando você navegar para o nó de Hospedagem, melhorando a experiência geral do usuário.

Suporte para HDX Plus para PCs em nuvem do Windows 365 e Desktops Virtuais do Azure. O Monitor agora oferece suporte a HDX Plus para Windows 365 PCs em nuvem e Desktops Virtuais do Azure (AVD). Para obter mais informações, consulte Solucionar problemas de máquinas.

Ambientes VDA com proxies para filtragem de internet e URL (Pré-visualização). Agora você pode usar o Serviço de Atualização de VDA para atualizar VDAs quando tiver proxies para conectividade com a internet e filtragem da web. O proxy configurado na política tem precedência sobre o proxy configurado no registro. Para obter mais informações, consulte Instalar VDAs. Além disso, consulte a lista de URLs que precisam ser incluídas na lista de permissões do proxy.

Alteração da Conta de Serviço do Cloud Build. O GCP está introduzindo alterações no comportamento padrão dos Serviços do Cloud Build e no uso de contas de serviço em novos projetos criados após April 29, 2024. Para obter mais informações, consulte Alteração da Conta de Serviço do Cloud Build. No entanto, seus projetos Google e catálogos Citrix existentes não são afetados por essa alteração. Para obter mais informações, consulte:

- Configurar e atualizar contas de serviço
- Permissões GCP necessárias

Março de 2024

Recursos novos e aprimorados

Gravação Dinâmica de Sessão. Agora você pode gravar a sessão ativa atual usando os controles de Gravação de Sessão na tela **Detalhes do Usuário** sem a necessidade de restabelecer a sessão. Esse recurso permite uma solução de problemas mais rápida e eficaz de problemas relacionados à experiência da sessão enfrentados pelos usuários. Isso é útil para depurar problemas difíceis de reproduzir.

Para obter mais informações sobre a Gravação Dinâmica de Sessão, consulte o artigo Serviço de Gravação de Sessão.

Ferramenta de registro para registrar VDAs usando WebSockets em catálogos de máquinas. Agora você pode usar essa ferramenta de registro para registrar com segurança seus VDAs não associados a domínio em catálogos de máquinas. Esse recurso oferece os benefícios de usar apenas a porta TLS 443 para comunicação do VDA com o Delivery Controller e remover o tráfego da porta 80. Para obter mais informações, consulte Registrar máquinas em catálogos usando a ferramenta de registro de VDA WebSocket.

Configuração Completa: Suporte para atualizar mais configurações de VM do Azure usando perfis de máquina. Com a Configuração Completa, agora você pode atualizar uma gama mais ampla de configurações para VMs do Azure provisionadas por MCS por meio de perfis de máquina, que incluem:

- Tamanho da máquina
- Tipo de licença
- Zona de Disponibilidade
- ID do Grupo de Host Dedicado

Após atualizar o perfil da máquina, a Configuração Completa compara as configurações atuais com as novas. Se houver diferenças, você será solicitado a confirmar quais aplicar. Este design garante atualizações transparentes e eficientes das configurações da VM.

Configuração Completa: Suporte para alteração das propriedades do cache de write-back para VMs do Azure provisionadas por MCS. Para VMs do Azure provisionadas usando o Machine Creation Services (MCS), agora você pode alterar suas propriedades de cache de write-back (WBC) usando a Configuração Completa, como **Tamanho do cache de disco**, **Tamanho do cache de memória** e **Habilitar economia de custo de armazenamento**. Além disso, ao selecionar um novo tamanho de máquina ou perfil de máquina para essas VMs, a Configuração Completa valida as configurações de WBC para evitar conflitos, como exceder o limite de memória da nova seleção. Se ocorrerem conflitos, você será solicitado a reconfigurar as configurações de WBC.

Fevereiro de 2024

Recursos novos e aprimorados

Suspender VMs da interface do Workspace. Agora você pode suspender VMs persistentes com sessões ativas a partir da interface do usuário do Workspace. Este aprimoramento oferece os seguintes benefícios:

- Retomar o sistema de onde você parou.

- Tempo de inicialização mais rápido em comparação com uma máquina parada e desalocada.
- Custo-benefício e eficiência energética.
- Alocação eficiente de recursos usando o recurso Autoscale.

Novo suporte para Otimização de Armazenamento do Machine Creation Services (MCS) (MCSIO): Agora você tem a opção de o Serviço de Portabilidade de Imagem adicionar ou remover o MCSIO ao preparar uma imagem para o provisionamento do MCS. Para obter mais informações, consulte Automatizar a configuração do VDA.

Aprimoramentos da Visão Geral de Probes: Um resumo das Métricas de Probe e dos Estágios de Falha de Probe está agora disponível na página **Probe** > **Visão Geral**. As Métricas de Probe mostram a contagem de execuções Agendadas, Falhas, Ignoradas e Bem-sucedidas. A representação gráfica dos estágios de falha ajuda a analisar os estágios em que a maioria das falhas ocorreu. Esta informação ajuda a solucionar rapidamente os resultados da probe. Para obter mais informações, consulte o artigo Sondagem de Aplicativos e Desktops.

Informações da imagem na página Catálogos de Máquinas. Agora você pode visualizar as seguintes informações da imagem através das **Propriedades do Modelo** do catálogo de máquinas:

- Sistema operacional
- Serviço de identidade da máquina
- Armazenamento do Machine Creation Service
- Caminho do arquivo para `pagefile.sys` para implantações do Azure

Este aprimoramento oferece maior clareza nas informações da imagem e garante que os administradores tenham todas as informações sobre o catálogo de máquinas em um só lugar.

Suporte de Configuração Completa para gerenciamento de token de registro de VDA. O registro de VDA baseado em token reduz a carga nos Cloud Connectors e diminui os pontos potenciais de falha, ideal para casos de uso em que você prepara as máquinas usando tecnologia de provisionamento não-Citrix. Com a Configuração Completa, agora você pode gerar e gerenciar tokens de registro para VDAs não provisionados pela Citrix, simplificando as implantações baseadas em token de registro. Para obter mais informações, consulte Gerar e gerenciar tokens de registro.

Registro do PowerShell. Na Configuração Completa, agora você pode visualizar os comandos do PowerShell correspondentes às suas ações diárias da interface do usuário. Este recurso ajuda você a obter insights sobre os comandos subjacentes do PowerShell para fins de aprendizado.

Para visualizar os logs do PowerShell, vá para **Registro > PowerShell**. Para obter mais informações, consulte Registro de configuração.

Habilitar Cache de Host Local (LHC) para VDAs agrupados de sessão única usando a Configuração Completa. Por padrão, os VDAs agrupados de sessão única provisionados usando MCS ou Citrix Provisioning ficam indisponíveis no modo LHC. Com a Configuração Completa, agora você pode substituir esse comportamento padrão por grupo de entrega, tornando esses VDAs disponíveis para novas conexões durante o LHC. Para obter mais informações, consulte Criar grupos de entrega e Gerenciar grupos de entrega.

Citrix Hypervisor™ renomeado para XenServer na Configuração Completa. Em linha com nossa estratégia de rebranding, atualizamos todas as instâncias de Citrix Hypervisor dentro da Configuração Completa para XenServer.

Visualização de salto de rede de ponta a ponta. A visualização de salto de rede de ponta a ponta é o próximo passo para aprimorar os fluxos de trabalho de solução de problemas no Citrix Monitor. A seção **Detalhes do Usuário** > **Desempenho da Sessão** > **Topologia da Sessão** fornece uma representação visual da visualização de salto de rede de ponta a ponta para sessões HDX conectadas. O caminho na sessão ajuda a entender os componentes envolvidos no caminho da sessão com seus metadados, o link entre os componentes e os aplicativos publicados no VDA. A Topologia da Sessão ajuda os fluxos de dados e a identificar o salto específico que pode estar causando problemas de desempenho.

Além disso, as medições de Latência ICA e RTT ICA são exibidas para a sessão quando ela está em um estado conectado. Para obter mais informações, consulte Visualização de salto de rede de ponta a ponta.

Usar o ID do Conjunto de Criptografia de Disco (DES ID) da imagem mestre para criptografar todos os discos das VMs do catálogo. Em ambientes Azure, anteriormente, o ID do Conjunto de Criptografia de Disco (DES ID) de um catálogo de máquinas MCS era derivado de um perfil de máquina ou de propriedades personalizadas. Com este recurso, um catálogo de máquinas também pode derivar o DES ID da imagem mestre para criptografar todos os discos das VMs em um catálogo.

Atualizar tags MCS para detectar recursos órfãos após a migração. Ao migrar de uma configuração local para um site na nuvem, ou de sua configuração na nuvem para outro site na nuvem, os recursos órfãos não são detectados corretamente devido à tag de ID do site antigo. Com este recurso, usando um comando PowerShell, você pode atualizar as tags de ID do site MCS de um catálogo persistente, após a migração, para que os recursos órfãos possam ser

detectados corretamente. Atualmente, este recurso é aplicável ao Azure. Para obter mais informações, consulte Atualizar tags MCS para detectar recursos órfãos após a migração.

Validar a configuração antes de criar um catálogo de máquinas MCS. Com este recurso, agora você pode validar as configurações antes de criar um catálogo de máquinas MCS usando o parâmetro `-validate` no comando `New-ProvScheme`. Depois de executar este comando PowerShell com o parâmetro, você receberá uma mensagem de erro apropriada se houver um parâmetro incorreto usado ou se um parâmetro entrar em conflito com outro. Você pode então usar a mensagem de erro para resolver o problema e criar com sucesso um catálogo de máquinas MCS usando o PowerShell.

Atualmente, este recurso é aplicável a ambientes de virtualização Azure, GCP e VMware. Para obter mais informações, consulte Validar a configuração antes de criar um catálogo de máquinas MCS.

Suporte para copiar tags de uma origem de perfil de máquina para uma VM no AWS. Com este recurso, em ambientes de virtualização AWS, você pode copiar tags em NICs e discos (disco de identidade, disco de cache de gravação e disco do SO) que são especificados no perfil da máquina para VMs recém-criadas em um catálogo de máquinas MCS. Você pode especificar essas tags em qualquer uma das origens de perfil de máquina (instância AWS EC2 ou versão de modelo de inicialização AWS). Este recurso é aplicável a catálogos de máquinas e VMs persistentes e não persistentes. Para obter mais informações, consulte Copiar tags em VMs.

Suporte SCVMM para perfil de máquina. Com este recurso, agora você pode usar um perfil de máquina para criar e atualizar um catálogo de máquinas MCS em ambientes do System Center Virtual Machine Manager (SCVMM). Você também pode habilitar a virtualização aninhada e o vTPM. Para obter mais informações, consulte Criar um catálogo com um perfil de máquina.

Suporte do Azure para usar VMs spot com MCS. As VMs Spot do Azure permitem que você aproveite a capacidade de computação não utilizada do Azure com uma economia significativa de custos. No entanto, devido à sua política de despejo, as VMs Spot do Azure são boas apenas para algumas aplicações e desktops não críticos.

Com este recurso, você pode criar um catálogo de máquinas MCS de VMs Spot do Azure usando um perfil de máquina (VM ou especificação de modelo). Você pode atualizar um catálogo existente para ter VMs Spot do Azure como as VMs recém-criadas ou mudar para ter VMs padrão do Azure. Você também pode atualizar VMs existentes para serem VMs Spot do Azure. Para obter mais informações, consulte Criar um catálogo usando VMs Spot do Azure.

Suporte para capturar configurações de diagnóstico de um perfil de máquina. Em ambientes Azure, o MCS agora oferece suporte à captura de configurações de diagnóstico em VMs e NICs de um perfil de máquina ao criar ou atualizar um catálogo de máquinas MCS, ou ao atualizar VMs existentes. Portanto, com esta implementação, os dados de diagnóstico podem ser transmitidos de forma contínua para endpoints de destino Azure designados, como workspaces do Log Analytics ou Event Hubs, para análise e visualização aprofundadas. Para obter mais informações, consulte Capturar configurações de diagnóstico em VMs e NICs de um perfil de máquina.

Suporte do MCS para gerenciar diferentes versões de um catálogo de máquinas. Com este recurso, você pode gerenciar as versões de configuração de um catálogo de máquinas usando comandos PowerShell. Cada alteração de configuração usando o `Set-ProvScheme` resulta em uma nova versão de configuração. Você pode:

- Ver a lista de versões.
- Usar qualquer versão anterior para atualizar um catálogo de máquinas.
- Excluir manualmente uma versão se ela não for usada por uma VM.
- Alterar o número máximo de versões a serem retidas por um catálogo de máquinas.

Para obter mais informações, consulte Gerenciar versões de um catálogo de máquinas.

Publicar aplicativos empacotados App-V, MSIX e MSIX app attach em VDAs de sessão única e desktop compartilhado. Agora você pode acessar aplicativos empacotados, por exemplo, App-V, MSIX e MSIX app attach em VDAs de sessão única e desktop compartilhado. Este aprimoramento garante que os aplicativos empacotados estejam prontamente disponíveis para uso quando você fizer login. Este recurso facilita o lançamento mais rápido de aplicativos empacotados e melhora significativamente sua experiência, aproximando-a do acesso a um aplicativo instalado localmente. Para obter mais informações, consulte Publicar aplicativos empacotados em VDAs de sessão única ou desktop compartilhado.

Reproduzir sessões ao vivo e gravadas: O Citrix Monitor agora oferece suporte à reprodução de sessões de usuário gravadas e ao vivo que são registradas usando o serviço de Gravação de Sessão. Você pode entender rapidamente os problemas relacionados à sessão encontrados pelo usuário a partir da reprodução. Com este recurso, você obtém acesso rápido às gravações, juntamente com métricas relacionadas à sessão, dentro do console do Monitor. Isso ajuda a correlacionar os problemas descobertos nas gravações com as métricas de desempenho. Elimina a necessidade de procurar gravações em vários servidores de gravação de sessão ou de procurar aplicativos de terceiros para visualizar as gravações.

Este recurso requer VDA e a versão 2308 ou posterior do servidor de Gravação de Sessão.

O Monitor armazena as gravações em um repositório centralizado e as exibe no modal **Seletor de Sessão**. O link **Sessões com gravações** exibe as gravações de sessões que estiveram ativas nas últimas 24 horas ou nos últimos 2 dias. A gravação é reproduzida em uma nova guia usando o servidor de reprodução do Citrix Session Recording.

Para obter mais informações, consulte Gravar sessões.

Otimização do Microsoft Teams: O Monitor exibe o status da otimização HDX disponível para o Microsoft Teams. A nova **Otimização do Microsoft Teams** pode ser visualizada na página **Detalhes do Usuário** > painel **Detalhes da Sessão**. O Monitor exibe o status da otimização do Microsoft Teams somente se o Microsoft Teams for executado como um aplicativo publicado ou dentro de um desktop publicado. Este aprimoramento fornece aos administradores visibilidade para permitir a solução de problemas de desempenho de sessão no Microsoft Teams relatados pelos usuários. Para obter mais informações, consulte Solucionar problemas do usuário.

Melhorias na interface do usuário: A interface do usuário do Citrix Monitor agora foi atualizada com uma aparência moderna. A nova e aprimorada interface do usuário oferece navegação mais fácil e melhor representação de dados. A experiência aprimorada é intuitiva e projetada para compreender facilmente os dados necessários para monitorar e solucionar problemas de uma sessão Citrix.

Resolução de tela ideal: A resolução de tela ideal recomendada para visualizar o Citrix Monitor foi atualizada para 1440 x 1024.

Janeiro de 2024

Recursos novos e aprimorados

Configuração aprimorada de redirecionamento de conteúdo bidirecional Anteriormente, a configuração do redirecionamento de conteúdo bidirecional envolvia o gerenciamento de três políticas distintas: Permitir redirecionamento de conteúdo bidirecional, Permitir redirecionamento de URLs para VDA e Permitir redirecionamento de URLs para o Cliente. Essas políticas exigem configurações tanto no lado do servidor (configuradas em **DaaS > Full Configuration**) quanto no lado do cliente (configuradas por meio de Políticas de Grupo). A partir desta versão, consolidamos todas as três políticas em uma única política unificada. Isso não apenas simplifica e aprimora o processo de configuração, mas também elimina a necessidade de configurações do lado do cliente. Para obter mais informações, consulte Configuração de redirecionamento de conteúdo bidirecional.

Suporte para reiniciar e desligar máquinas de sessão única na guia Sessões do nó Pesquisar. Na guia **Sessões** do nó **Pesquisar**, agora você pode procurar sessões de usuário em um estado não íntegro e reiniciar ou desligar facilmente as máquinas de sessão única associadas na mesma guia. Esse recurso aumenta a eficiência, permitindo uma ação rápida sobre os problemas de sessão identificados em uma única interface.

Suporte para acessar o Global App Configuration Service a partir da Configuração Completa. Fornecemos itens de ação na interface de Configuração Completa para vinculá-lo ao Global App Configuration Service. Com essa integração, você pode acessar facilmente o Global App Configuration para gerenciar as configurações do usuário final por meio da Configuração Completa.

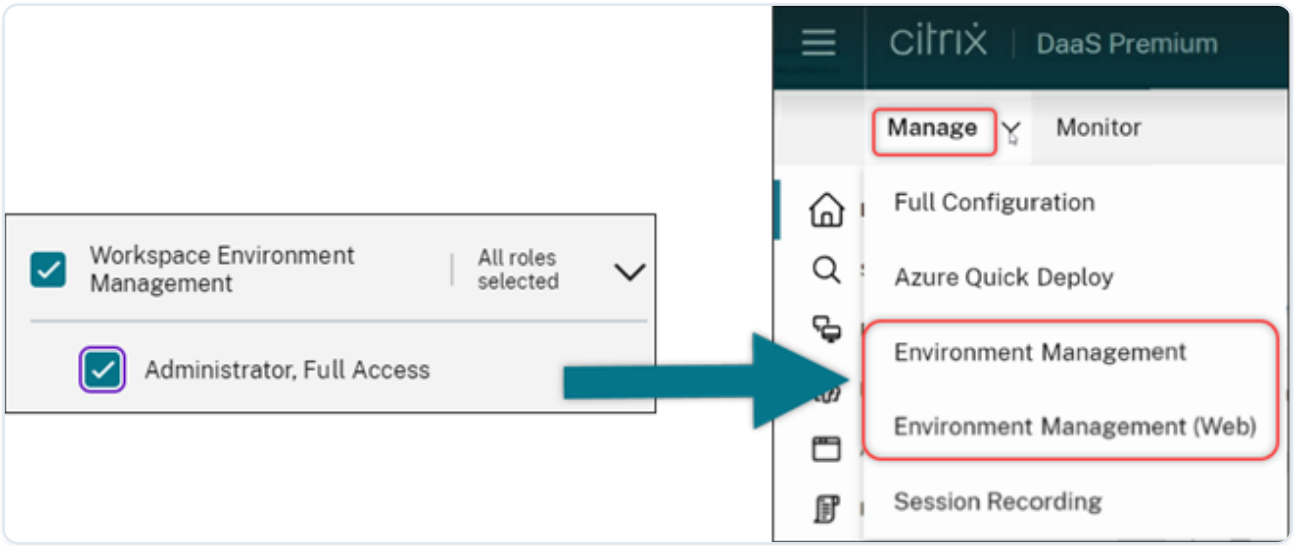
Para acessar este serviço a partir da Configuração Completa, você tem duas opções:

- Selecione o nó **StoreFront**, clique em um registro de servidor e, em seguida, selecione **Configurar Configurações do Cliente** na barra de ações.
- Selecione o nó **Políticas** e, em seguida, selecione **Configurar Configurações do Cliente** na barra de ações.

Suporte para gerenciar atribuições de usuário para grupos de entrega gerenciados pelo Citrix Cloud usando a Configuração Completa. Como parte do nosso plano para migrar o gerenciamento de atribuições de usuário da Biblioteca da Nuvem para a Configuração Completa, agora você pode gerenciar atribuições de usuário para grupos de entrega gerenciados pelo Citrix Cloud por meio da Configuração Completa. Para realizar essa tarefa, edite um grupo de entrega de destino em **Configuração Completa > Grupos de Entrega** e designe os usuários permitidos a usar desktops ou aplicativos por meio de um destes menus: **Desktops** (ou **Regras de Atribuição de Desktop**) ou **Regra de Atribuição de Aplicativo**. Para obter mais informações, consulte Gerenciar grupos de entrega.

As atualizações feitas em um portal são sincronizadas perfeitamente com o outro, garantindo atualizações consistentes em ambos os portais.

Limitar o acesso ao console WEM à função de Administrador de Acesso Total do WEM. Habilitamos o controle de acesso para os consoles do Workspace Environment Management™ (WEM) para evitar entrada não autorizada. Somente usuários com a função de **Administrador de Acesso Total do Workspace Environment Management** agora podem usar **DaaS > Gerenciar** para acessar os consoles WEM.



Configuração Completa: Suporte para catálogos do Azure herdarem configurações DES de imagens mestre. Anteriormente, a Configuração Completa definia as configurações DES padrão dos catálogos do Azure apenas com base em perfis de máquina. Agora expandimos essa capacidade. Com esse aprimoramento, nos seguintes casos, a Configuração Completa define as configurações DES padrão de um catálogo do Azure diretamente com base na imagem mestre:

- Se um perfil de máquina não for selecionado
- Se o perfil especificar uma Chave Gerenciada pela Plataforma (PMK)

Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager na interface de Configuração Completa.

Pesquisa aprimorada: Mais filtros para maior precisão. Aprimoramos a pesquisa no nó Pesquisa para incluir dois novos filtros, Zona e Tipo de Provisionamento, para maior precisão e usabilidade aprimorada.

Configuração Completa: Suporte para seleção do tipo de máquina do Google Cloud para catálogos de máquinas GCP. Com este recurso, os administradores têm a flexibilidade de selecionar as configurações de memória e processador necessárias para VMs GCP provisionadas, adaptando-as para atender a requisitos operacionais específicos. Para obter mais informações, consulte Criar um catálogo de máquinas usando a interface de Configuração Completa.

Suporte para chaves de criptografia gerenciadas pelo cliente (CMEK) globais e regionais para provisionamento de VMs GCP. Agora você pode usar chaves CMEK globais e regionais para provisionar VMs de qualquer projeto de provisionamento. Este aprimoramento oferece maior flexibilidade na seleção de chaves para provisionamento de VMs e melhora a segurança das VMs.

Dezembro de 2023

Recursos novos e aprimorados

Progresso do Envio de Mensagens. Agora você pode visualizar o progresso da operação **Enviar Mensagem** disponível em **Monitor** > **Filtros**. Esta operação ajuda a enviar mensagens em massa para todas as sessões conectadas em seu Site. O progresso da operação é exibido em porcentagem. Uma vez concluída a operação, o sistema exibe o número de mensagens que foram enviadas e o número que falharam. O status de envio de mensagens é útil ao administrar sites grandes. Ajuda a entender se a mensagem precisa ser reenviada a certos usuários. O envio de mensagens pode falhar se as máquinas estiverem não registradas ou se as sessões estiverem com falha. Para obter mais informações sobre Enviar Mensagem, consulte Enviar mensagens para usuários.

Suporte à autenticação do Citrix Probe Agent via Citrix Gateway com credenciais de domínio e autenticação multifator.

O Citrix Probe Agent para sondagem de aplicativos e desktops agora oferece suporte à autenticação via Citrix Gateway com credenciais de domínio e autenticação multifator. Este recurso ajuda a executar o Probe Agent em máquinas conectadas ao StoreFront via Citrix Gateway. Os resultados abrangentes da sondagem disponíveis no Monitor ajudam a solucionar problemas relacionados a aplicativos, máquina host ou conexão antes que os usuários os experimentem. O suporte para Citrix Gateway com autenticação multifator está disponível apenas para Citrix Gateway configurado com LDAP e OTP Nativo usando o Esquema de Login Único. Para obter mais informações, consulte Sondagem de Aplicativos e Desktops

Interface de usuário da Política de Acesso redesenhada para controle de acesso a recursos mais flexível. Redesenhamos a interface de usuário **Editar grupo de entrega > Política de Acesso** para oferecer mais flexibilidade no gerenciamento do acesso a recursos para grupos de entrega. A seguir estão os principais recursos disponíveis com o novo design:

- **Suporte para adicionar políticas.** Agora você pode adicionar políticas de acesso para restringir o acesso a recursos com base nos atributos das conexões do usuário. Uma política pode consistir em dois tipos de critérios:
  - **Critérios de inclusão.** Permitem especificar as conexões de usuário que têm permissão para acessar o grupo de entrega.
  - **Critérios de exclusão.** Permitem especificar as conexões de usuário que estão proibidas de acessar o grupo de entrega.

- **Suporte a filtros expandido.** Agora você pode definir critérios de inclusão e exclusão usando uma variedade de filtros SmartAccess. Esses filtros incluem filtros de Workspace, como `Citrix.Workspace.UsingDomain` e `Citrix-Via-Workspace`, bem como filtros para acesso adaptativo baseado na localização da rede.
- **Suporte à lógica 'Corresponder a Todos' para critérios incluídos.** A nova lógica permite que você alcance um alto nível de precisão e controle ao especificar conexões de usuário permitidas para grupos de entrega.

Para obter mais informações, consulte Restringir o acesso a recursos em um grupo de entrega.

Novembro de 2023

Recursos novos e aprimorados

Suporte para a criação de catálogos do Citrix Provisioning usando a interface de Configuração Completa. Para criar um catálogo do Citrix Provisioning, você precisava usar o Assistente de Configuração do Citrix Virtual Apps and Desktops. Com este recurso, agora você pode criar um catálogo do Citrix Provisioning usando a interface de Configuração Completa e o PowerShell.

Esta implementação oferece as seguintes vantagens:

- Um único console unificado para gerenciar catálogos MCS e Citrix Provisioning.
- Possui novos recursos para catálogos do Citrix Provisioning, como solução de gerenciamento de identidade, provisionamento sob demanda e assim por diante.

Atualmente, este recurso está disponível apenas para cargas de trabalho do Azure. Para obter mais informações, consulte Criar catálogos do Citrix Provisioning no Citrix Studio.

Introdução da pesquisa para Grupos de Aplicativos. Introduzimos a funcionalidade de pesquisa para grupos de aplicativos no nó **Aplicativos**. Com este aprimoramento, agora você pode pesquisar diretamente um grupo de aplicativos dentro de qualquer pasta de aplicativo. Para obter mais informações, consulte Pesquisar Grupos de Aplicativos.

Limites de configuração modificados. A tabela a seguir descreve as modificações feitas nos limites de configuração do DaaS para melhorar o desempenho e proporcionar economia de custos.

RECURSO	LIMITE ANTIGO	NOVO LIMITE
Domínios do Active Directory	85	100

RECURSO	LIMITE ANTIGO	NOVO LIMITE
Catálogos	1000	2000
Grupos de Entrega	1000	2000
Localização do recurso	85	100
Localização do recurso -> Total de sessões	20.000	25.000

Para obter mais informações, consulte Limites.

Uma única opção para reter a VM e o disco do sistema durante os ciclos de energia. Iniciar uma VM existente no Azure agora é mais rápido do que iniciar uma nova, tornando-a uma escolha mais eficiente para reter VMs entre os ciclos de energia. Em resposta a essa mudança, combinamos as opções **Reter VMs entre ciclos de energia** e **Reter disco do sistema durante ciclos de energia** em uma única opção **Reter VM e disco do sistema durante ciclos de energia**. Isso significa que, ao selecionar esta opção para reduzir os tempos de reinício da VM, retendo os discos do sistema, suas VMs também são retidas.

Nova capacidade na Configuração Completa para filtrar tamanhos de máquina com base na *propriedade Criptografia no Host* em perfis de máquina (específico para VMs do Azure). Depois de escolher um perfil de máquina com *Criptografia no Host* ativada durante a criação ou gerenciamento de catálogo de máquinas do Azure, apenas os tamanhos de máquina que suportam esse recurso são exibidos.

Restringir ações de backup e restauração à função de Administrador Completo. Aprimoramos o controle de acesso para as ações de backup e restauração. Somente usuários com a função de Administrador Completo agora podem acessar o nó **Backup + Restauração**, evitando ações não autorizadas.

Cache de dados para o nó Pesquisa. Introduzimos o cache de dados para o nó **Pesquisa** do Citrix DaaS. Este aprimoramento melhora o desempenho da pesquisa e a seguir lista os casos de uso que facilitam suas tarefas regulares:

- Exibição rápida dos resultados da pesquisa após serem recuperados pela primeira vez.
- Retém os resultados da paginação após navegar para fora e voltar para o nó **Pesquisa**.

Informações da imagem na página Catálogos de Máquinas. Agora você pode visualizar as seguintes informações da imagem através das **Propriedades do Modelo** do catálogo de máquinas:

- Sistema operacional
- Serviço de identidade da máquina
- Armazenamento do Machine Creation Service
- Caminho do arquivo para `pagefile.sys` para implantações do Azure.

Este aprimoramento oferece maior clareza sobre as informações da imagem e garante que os administradores tenham todas as informações sobre o catálogo de máquinas em um só lugar.

Suporte para fixar filtros de pesquisa. Para proporcionar uma experiência de pesquisa rápida, a Configuração Completa permite fixar seus filtros de pesquisa. Os fixadores de filtro permitem que você mantenha os filtros de pesquisa usados com frequência acessíveis na página. Este aprimoramento está disponível nos painéis de pesquisa dos seguintes nós:

- **Pesquisa**
- **Catálogos de Máquinas**
- **Grupos de Entrega**
- **Aplicativos**

Para obter mais informações, Use a Pesquisa na interface de gerenciamento de Configuração Completa.

Suporte para associar metadados a logs de configuração. Usando este aprimoramento, agora você pode anexar metadados aos logs de configuração associando um par `name-value` nas operações de alto nível. Para obter mais informações, consulte Associar metadados a logs de configuração.

Ignorar recursos órfãos com tag específica. Em ambientes Azure, um recurso gerenciado pelo cliente e marcado com todas as tags Citrix é detectado como um recurso órfão. Com este recurso, se você adicionar outra tag `CitrixDetectIgnore` com valor true a esse recurso, o recurso será ignorado ao detectar recursos órfãos.

Solução para o problema de GUID duplicado do SCCM. Após criar várias VMs usando o MCS, o System Center Configuration Manager (SCCM) exibia apenas uma VM em seu console devido a GUIDs duplicados. Este problema agora é resolvido adicionando uma etapa na preparação da

imagem. Esta etapa exclui os certificados existentes e as informações de GUID dentro da imagem mestre. A etapa é habilitada por padrão.

Reparar as informações de identidade de contas de computador ativas. Com este recurso, você pode redefinir as informações de identidade de contas de computador ativas que apresentam problemas relacionados à identidade. Você pode optar por redefinir apenas a senha da máquina e as chaves de confiança, ou redefinir toda a configuração do disco de identidade. Esta implementação é aplicável a catálogos de máquinas persistentes e não persistentes. Atualmente, o recurso é suportado apenas para ambientes de virtualização Azure e VMware. Para obter mais informações, consulte Reparar as informações de identidade de contas de computador ativas.

Obter informações de criptografia no host associadas a um perfil de máquina. Em ambientes Azure, com este recurso, agora você pode saber se a criptografia no host está habilitada para uma entrada de perfil de máquina (VM ou especificação de modelo) usando comandos PowerShell. Para obter mais informações, consulte Recuperar informações de criptografia no host de um perfil de máquina.

Reparar os certificados de usuário de identidades de máquina unidas ao Azure AD híbrido. Com este recurso, você pode usar o comando Powershell para reparar os certificados de usuário de identidades de máquina unidas ao Azure AD híbrido, caso estejam corrompidos ou expirem. Para obter mais informações, consulte Pool de identidades de máquina unida ao Azure Active Directory híbrido.

Suporte para aviso de expiração de certificado para catálogos de máquinas unidas ao Azure AD híbrido. A Configuração Completa agora fornece avisos com um mês de antecedência para a expiração de certificados de usuário em catálogos de máquinas unidas ao Azure AD híbrido. Este aprimoramento visa reduzir o risco de interrupções de serviço resultantes da expiração do certificado. Para visualizar os detalhes e as ações recomendadas, vá para o nó **Catálogos de Máquinas**, selecione o catálogo de máquinas e clique na guia **Solução de Problemas**.

Você pode executar o comando `Get-ProvScheme` para obter informações sobre a data de expiração do certificado de usuário de um catálogo de máquinas unidas ao Azure AD híbrido.

Suporte para VMs confidenciais do Azure (Pré-visualização). As VMs de computação confidencial do Azure garantem que seu desktop virtual seja criptografado na memória e protegido em uso. Com este recurso, agora você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho de perfil de máquina para criar tal catálogo. Você pode usar tanto VM quanto especificação de modelo ARM como entrada de perfil

de máquina. Para obter mais informações, consulte VMs confidenciais do Azure (Pré-visualização).

Suporte para converter um catálogo de máquinas não baseado em perfil de máquina para um baseado em perfil de máquina em ambiente AWS. Em um ambiente AWS, agora você pode usar uma VM ou um modelo de inicialização como entrada de perfil de máquina para converter um catálogo de máquinas que não utiliza perfis de máquina para um que adota essa abordagem. Novas VMs adicionadas ao catálogo herdam os valores de propriedade do perfil de máquina. Para obter mais informações, consulte Converter um catálogo de máquinas não baseado em perfil de máquina para um baseado em perfil de máquina.

Suporte para plug-in HPE Moonshot gerenciado pela Citrix (Pré-visualização). Anteriormente, você usava o plug-in Moonshot gerenciado pela HPE (HPE Moonshot Machine Manager) mantido pela Hewlett Packard Enterprise (HPE) para realizar as ações de gerenciamento de energia em chassis HPE Moonshot. O plug-in era baseado em APIs legadas que dificultavam os projetos de infraestrutura do MCS. Com este recurso, um plug-in HPE Moonshot gerenciado pela Citrix (HPE Moonshot) é introduzido. Com este plug-in, você pode criar conexões com seu chassis HPE Moonshot, criar catálogos e gerenciar a energia das máquinas no catálogo usando a interface de Configuração Completa e comandos PowerShell. Para obter mais informações, consulte:

- Ambientes de virtualização HPE Moonshot (Prévia)
- Conexão com HPE Moonshot (Prévia)
- Criar um catálogo de máquinas HPE Moonshot (Prévia)
- Gerenciar um catálogo HPE Moonshot (Prévia)

Capacidade de alterar o tamanho da memória e do cache de disco. Com este recurso, agora você pode alterar o tamanho da memória e do cache de disco do cache de Write-back (quando o MCSIO está habilitado) usando um comando PowerShell sem criar um novo catálogo de máquinas. Essa implementação ajuda você a ter a configuração de cache otimizada que é adequada para as suas necessidades de negócios. Este recurso é aplicável a:

- Ambientes GCP e Microsoft Azure, e
- um catálogo não persistente com MCSIO habilitado

Para obter mais informações, consulte Alterar a configuração do cache em um catálogo de máquinas existente.

Suporte para a criação de um catálogo habilitado para chave de criptografia gerenciada pelo cliente. Em ambientes Azure, agora você pode criar um catálogo do Citrix Provisioning

habilitado com chave de criptografia gerenciada pelo cliente (CMEK) usando a interface de Configuração Completa e comandos PowerShell. Para obter mais informações, consulte Criar um catálogo habilitado para chave de criptografia gerenciada pelo cliente.

Capacidade de copiar tags em todos os recursos no Azure. Com este recurso, no ambiente Azure, agora você pode copiar tags especificadas em um perfil de máquina para todos os recursos, como várias NICs e discos (disco do SO, disco de identidade e disco de cache de write-back) de uma nova VM ou de uma VM existente em um catálogo de máquinas.

A origem do perfil da máquina pode ser uma VM ou uma especificação de modelo ARM. Para obter mais informações, consulte Copiar tags em todos os recursos.

Estado da sessão atualizado para desconectado após a suspensão da máquina. Anteriormente, depois de suspender uma VM, a sessão ainda era exibida como **Ativa**. Com este aprimoramento, depois de suspender uma VM, o estado da sessão associada agora é exibido como **Desconectada**.

Suporte para a criação de VMs AWS que suportam hibernação. Agora você pode criar catálogos de máquinas que suportam a hibernação de VMs em seus ambientes AWS, aumentando a relação custo-benefício geral de sua implantação. Você também pode editar um catálogo para incluir VMs com capacidade de hibernação se o perfil de máquina associado suportar essa capacidade. Para obter mais informações, consulte Gerenciar energia de VMs AWS.

Suporte para configurar métodos de balanceamento de carga no nível do grupo de entrega (Prévia). Este recurso permite que você escolha o método de **Balanceamento de Carga Vertical** no nível do grupo de entrega. Com este recurso, cada máquina é alinhada ao índice de carga máximo antes que a próxima máquina seja ligada. O Autoscale e o Balanceamento de Carga Vertical determinam quando a próxima máquina é ligada. Este recurso alcança a utilização máxima para cada máquina e economia de custos em nuvens públicas. Este recurso oferece mais flexibilidade no gerenciamento das estratégias de balanceamento de carga para máquinas.

Você pode configurar um grupo de entrega para herdar o método de balanceamento de carga das configurações de nível de site ou substituir o método de balanceamento de carga de nível de site e, em vez disso, escolher um dos métodos de balanceamento de carga vertical ou horizontal. Para obter mais informações, consulte Etapa 2. Balanceamento de carga.

Suporte para VMs com capacidade de hibernação no Azure (Pré-visualização). Em ambientes Azure, você pode criar um catálogo de máquinas MCS que suporta hibernação. Usando este recurso, você pode suspender uma VM e, em seguida, reconectar-se ao estado

anterior da VM quando um usuário fizer login novamente. Para obter mais informações, consulte Criar VMs com capacidade de hibernação (Pré-visualização).

Guia de introdução do DaaS. Lançamos um novo guia para otimizar e simplificar a implantação e configuração do DaaS para administradores novos e experientes. Ele oferece estes principais benefícios:

- **Fácil de começar.** Usando uma abordagem passo a passo baseada em questionário, este guia ajuda novos administradores a configurar suas implantações rapidamente. As informações de ajuda contextual em todo o guia auxiliam na compreensão de conceitos e terminologia essenciais.
- **Simplifique configurações complexas.** Este guia inclui configurações pré-configuradas onde aplicável e fornece acesso à interface do usuário de Configuração Completa para configuração avançada. Administradores experientes podem usá-lo como base para configurações mais complexas.

Para obter mais informações, consulte Usar o guia de introdução do DaaS.

Atribuir letras de unidade a discos de cache de write-back usando a Configuração Completa. Anteriormente, você só podia atribuir uma letra de unidade específica ao disco de cache de write-back usando um cmdlet do PowerShell. Agora você pode realizar a mesma tarefa usando a Configuração Completa. Para obter mais informações, consulte Criar catálogos de máquinas.

Suporte para alterar várias propriedades de máquina Azure usando a Configuração Completa. Para máquinas Azure provisionadas pelo Machine Creation Services, agora você pode alterar as seguintes configurações de propriedade usando a Configuração Completa:

- Tipo de armazenamento
- Grupo de host dedicado
- Configurações da Galeria de Computação do Azure

Ao alterar qualquer uma dessas configurações, a Configuração Completa identifica automaticamente as configurações relacionadas e fornece sincronização automática ou mensagens de prompt solicitando que você selecione novamente as configurações relacionadas. Essa capacidade garante alterações consistentes em todas as configurações associadas, evitando possíveis erros de configuração. Para obter mais informações, consulte Editar um catálogo.

Usar pools de identidade existentes para criar identidades para máquinas provisionadas por MCS. Ao criar catálogos unidos ao AD ou adicionar máquinas a eles usando a Configuração Completa, agora você pode usar um pool de identidade existente para alocar identidades de máquina. Esse recurso permite aplicar um esquema de nomenclatura de conta de máquina consistente em vários catálogos. Para obter mais informações, consulte Identidades de máquina.

Topologia da Sessão. A visualização Topologia da Sessão é o próximo passo para aprimorar os fluxos de trabalho de solução de problemas no Monitor. A visualização Topologia da Sessão fornece uma representação visual do caminho na sessão para sessões HDX conectadas. Você pode acessar a visualização de topologia em **Detalhes do Usuário > Desempenho da Sessão**.

A visualização Topologia da Sessão para uma sessão HDX conectada mostra os componentes envolvidos no caminho da sessão com seus metadados, o link entre os componentes e os aplicativos publicados no VDA. Além disso, as medições de Latência ICA e RTT ICA são exibidas para a sessão quando ela está em um estado conectado.

Use a visualização Topologia da Sessão para entender os componentes pelos quais os dados da sessão fluem e para identificar o salto específico que pode estar causando problemas de desempenho. Para obter mais informações, consulte Topologia da Sessão.

Outubro de 2023

Recursos novos e aprimorados

Ajuste suas configurações de Autoscale usando o uso histórico. Uma nova guia de configurações do Autoscale chamada **Autoscale Insights**, oferece um gráfico abrangente que compara visualmente suas configurações de Autoscale e os dados de uso da máquina da semana anterior. Com este gráfico, você pode obter insights sobre a eficácia das configurações do Autoscale:

- **Não é econômico**. Há desperdício financeiro devido ao provisionamento excessivo de capacidade.
- **Experiência do usuário ruim**. A experiência do usuário é impactada negativamente devido ao provisionamento insuficiente de capacidade.
- **Bom equilíbrio entre experiência do usuário e custo**. A capacidade provisionada está alinhada com o uso histórico.

Para obter mais informações, consulte Analisar a eficácia das configurações do Autoscale.

Suporte a várias NICs para VMs do Azure. Com a Configuração Completa, agora você pode criar VMs do Azure com várias NICs. A contagem máxima de NICs de uma VM é determinada pela configuração de tamanho da máquina, enquanto sua contagem real de NICs permitida é definida pela configuração do perfil da máquina. Para obter mais informações, consulte Criar catálogos de máquinas.

Para criar ou atualizar um catálogo com várias NICs por VM usando comandos do PowerShell, consulte Criar ou atualizar um catálogo com várias NICs por VM.

Tendências para métricas de desempenho da sessão. O Monitor está introduzindo uma nova guia **Detalhes do Usuário > Desempenho da Sessão** com fluxos de trabalho de solução de problemas aprimorados, começando com a capacidade de correlacionar métricas em tempo real na identificação de problemas dentro das sessões do usuário. A Experiência da Sessão agora contém tendências de métricas de sessão como ICARTT, Latência ICA, Quadros por Segundo, Largura de Banda de Saída Disponível e Largura de Banda de Saída Consumida. Este recurso ajuda a reduzir o tempo médio de resolução, permitindo que você correlacione várias métricas de desempenho em uma única visualização. Para obter mais informações, consulte o artigo Problemas do Usuário.

Suporte à versão do VDA na página de configurações de criação/edição de política. Como parte da criação de uma política, ao configurar as definições, o sistema oferece uma opção para visualizar o tipo de definição. Você pode visualizar os seguintes tipos de definição:

- Todas as configurações - Visualizar todas as configurações para todas as versões do VDA
- Somente configurações atuais - Visualizar configurações apenas para as versões atuais do VDA
- Somente configurações legadas - Visualizar configurações apenas para as versões VDA obsoletas

Para obter mais informações, consulte Criar políticas

Visibilidade de aplicativo limitada suportada apenas para contas do Active Directory. A capacidade de limitar a visibilidade do aplicativo está disponível apenas para contas de usuário do Active Directory, e não para contas do Azure Active Directory e Okta. Observe que, para auxiliar esse recurso, no fluxo de trabalho de configuração do aplicativo, na página Selecionar Usuários ou Grupos, as opções **Azure Active Directory** e **Okta** no campo **Selecionar tipo de identidade** estão desabilitadas.

Nova opção de UI para excluir registros de VM apenas do banco de dados do site Citrix. Quando a exclusão de catálogo e VM falha devido a um hipervisor inacessível, agora você pode optar por excluir apenas os registros de VM do banco de dados do site Citrix, deixando as VMs intactas no host. Para obter mais informações, consulte Excluir um catálogo.

Suporte para a criação de catálogos de máquinas vazios para máquinas não provisionadas por MCS. A criação de catálogos de máquinas vazios agora se estende a máquinas não provisionadas por MCS, incluindo:

- Máquinas virtuais ou blade provisionadas usando tecnologias diferentes do Machine Creation Services.
- Máquinas físicas não gerenciadas por energia pelo Citrix DaaS
- Máquinas de Acesso Remoto a PC

Com esse recurso, agora você pode criar catálogos de máquinas sem a necessidade de adicionar máquinas a eles durante a criação do catálogo.

Aprimoramentos na Atualização de Imagem. Anteriormente, ao atualizar imagens, todas as imagens na árvore de imagens eram atualizadas, independentemente de um nó específico na árvore ter sido selecionado. Com o aprimoramento mais recente, se você selecionou um nó, apenas as imagens nesse nó são atualizadas. Esse aprimoramento garante um processo de atualização mais direcionado, melhorando significativamente a velocidade de atualização da imagem. Além disso, agora você pode desmarcar um nó selecionado na árvore de imagens mantendo CTRL pressionado e clicando no nó. Para obter mais informações, consulte Imagem mestre.

Autoscale de Pico Atribuído Ligado. Quando os desktops persistentes são ligados, mas permanecem sem uso ou se nenhum usuário faz logon, os administradores podem definir o tempo de espera para realizar ações como, nenhuma ação, suspender ou desligar.

Para máquinas atribuídas, onde ela está ligada, mas uma sessão não foi conectada a ela dentro do tempo definido após o início do horário de pico, você pode adicionar uma política no nível do grupo de entrega para desligar a máquina.

Para máquinas atribuídas, onde ela está em estado de retomada, mas uma sessão não foi conectada a ela dentro do tempo definido após o início do horário de pico, você pode adicionar uma política no nível do grupo de entrega para suspender a máquina.

Esse recurso é útil se houver um usuário final de licença, ou que não fez logon, ou se uma empresa tiver um feriado prolongado, então você pode definir o tempo de espera e as ações de

desconexão da máquina a serem tomadas para ajudar a reduzir o custo de consumo do Azure. Para obter mais informações, consulte Grupos de entrega aleatórios de SO de sessão única e Grupos de entrega estáticos de SO de sessão única.

Monitorar várias instâncias do Citrix DaaS (Pré-visualização). Agora você pode usar o Citrix Monitor para monitorar e solucionar problemas em várias instâncias do Citrix DaaS. O Citrix DaaS permite que os clientes agreguem várias instâncias de serviço usando um modelo de hub e spoke. Com essa configuração, os administradores podem realizar pesquisas de helpdesk em todas as instâncias DaaS configuradas a partir de um único console do Monitor. Para obter mais informações sobre a configuração necessária para agregar as instâncias de serviço spoke a um hub, consulte Agregar várias instâncias de serviço do Citrix Virtual Apps and Desktops. O Monitor suporta a agregação de até quatro locatários DaaS (spokes) sob um único locatário DaaS (hub). Para ter monitoramento unificado em todos os locatários DaaS, use a enumeração bidirecional das instâncias de hub e spoke. Para obter mais informações, consulte Pesquisa Agregada em várias instâncias DaaS (Pré-visualização).

Suporte para vSAN 8.0. Agora você pode usar o MCS para provisionar VMs no ambiente vSAN 8.0.

Preservar configurações de NIC em VMs provisionadas. Anteriormente, as configurações de NIC da imagem mestre não eram retidas nas VMs provisionadas. Por exemplo, se você configurasse as configurações de DNS na imagem mestre, as VMs provisionadas não reteriam as configurações de DNS configuradas da imagem mestre. Com esse recurso, as VMs provisionadas agora podem reter as configurações de NIC da imagem mestre. As configurações são retidas mesmo após uma atualização do Windows. O driver de filtro é instalado automaticamente se você fizer uma instalação limpa do VDA versão 2308 ou posterior em uma máquina implantada no Hyper-V por meio das instalações da imagem mestre do MCS. No entanto, atualmente, se você atualizar de uma versão mais antiga do VDA (versão inferior a 2308) e quiser instalar o driver de filtro, deverá selecionar a caixa de seleção **Citrix HyperV Filter Driver** na página **Componentes Adicionais** ao atualizar o VDA. Para obter mais informações, consulte Instalar componentes adicionais.

Este recurso é aplicável a:

- VMs Hyper-V (incluindo Azure e SCVMM)
- Catálogos de máquinas MCS persistentes e não persistentes
- Catálogos de máquinas MCS não persistentes com MCSIO
- Imagem mestre com várias NICs

Detectar recursos órfãos do Azure. Com este recurso, agora você pode detectar os recursos órfãos em sua implantação do Azure, permitindo um gerenciamento eficiente de recursos. Depois que os recursos órfãos são identificados, você pode tomar outras ações, trazendo mais produtividade e redução de custos. Para obter mais informações, consulte Detectar recursos órfãos do Azure em sua implantação.

Novo status de atualização de imagem. Ao monitorar os status de atualização de imagem para catálogos na Configuração Completa, agora você pode visualizar um novo status **Preparando imagem**, além dos existentes **Totalmente atualizado**, **Parcialmente atualizado** e **Atualização pendente**. Para obter mais informações, consulte Alterar a imagem mestre.

Comandos PowerShell para criar Auto-tags (Pré-visualização). Com este recurso, agora você pode criar tags automaticamente usando o comando PowerShell. Para obter mais informações, consulte Auto Tags.

Sinal de notificação é exibido para o usuário ou grupo de entrega. Ao criar ou modificar uma política e configurar as definições, se todos os grupos de entrega estiverem desabilitados, o sistema exibe um aviso de que - Nenhum dos elementos neste filtro está habilitado. Se pelo menos um grupo de entrega estiver habilitado, o sistema não exibe o sinal de aviso. Para obter mais informações, consulte Configurações de política

Setembro de 2023

Recursos novos e aprimorados

Comandos PowerShell para gerenciar o Local Host Cache (LHC). Agora você pode usar comandos PowerShell para gerenciar o LHC nos Citrix Cloud Connectors. Para obter mais informações, consulte Comandos PowerShell do Local Host Cache.

Suporte para criação de catálogos de máquinas vazios. Na Configuração Completa, agora você pode criar um catálogo de máquinas sem a criação imediata de VMs. Com este recurso, você pode adiar a criação de VMs até que os hosts de back-end estejam totalmente preparados ou o provisionamento de VMs seja concluído, ganhando mais flexibilidade na criação de catálogos. Atualmente, este recurso se aplica apenas a catálogos provisionados pelo Machine Creation Services. Para obter mais informações, consulte Criar catálogos de máquinas.

Cache de dados para o nó Home. Introduzimos o cache de dados para o nó **Home** do Citrix DaaS. Este aprimoramento melhora a experiência do usuário, reduzindo os tempos de carregamento da página quando você navegar para o nó **Home**.

Aprimoramentos de pesquisa para aplicativos. Reformulamos a funcionalidade de pesquisa no nó **Aplicativos** para alinhar com o novo design introduzido no nó **Pesquisa**. Este novo recurso melhora sua experiência de pesquisa de aplicativos e mantém uma experiência de pesquisa consistente em todo o DaaS. A palavra-chave **Nome do Aplicativo** na expressão de filtro é renomeada para **Nome**, mantendo seu significado original. Para obter mais informações, consulte Usar Pesquisa na interface de gerenciamento de Configuração Completa.

Gerenciamento de escopo aprimorado: exibição de objetos em visualização de pasta. Nas páginas de criação e gerenciamento de escopo, os catálogos de máquinas, grupos de entrega e grupos de aplicativos agora são exibidos em estruturas de pastas que se alinham com seu gerenciamento no DaaS. Essa visualização de pasta simplifica o processo de seleção de objetos para criação e gerenciamento de escopo, tornando suas escolhas mais intuitivas e diretas. Para obter mais informações, consulte Criar e gerenciar escopos.

Removida a opção Deixar o gerenciamento de usuários para o Citrix Cloud. Ao criar um grupo de entrega em Gerenciar > Configuração Completa, na página Usuários, o suporte para esta opção foi removido. Para grupos de entrega onde as atribuições de usuário foram tratadas através do Citrix Cloud, continue a gerenciar as atribuições de usuário dentro da biblioteca do Citrix Cloud.

Removida a opção Azure Germany. Em linha com o encerramento do Microsoft Cloud Deutschland em October 29, 2021, removemos a opção **Azure Germany** da página de criação de conexão de host.

Alertas de serviço proativos na Configuração Completa. Os alertas são apresentados em dois níveis — alertas em todo o site mostrados em Início (ícone de bandeira) e alertas relacionados à zona mostrados na guia Solução de problemas de cada zona. Atualmente, esse recurso fornece avisos e alertas proativos para garantir que seu Local Host Cache e suas zonas estejam configurados corretamente para que, quando ocorrer uma interrupção, o Local Host Cache funcione e seus usuários não sejam afetados. Para obter mais informações, consulte Alertas de integridade do serviço e Zonas.

Agosto de 2023

Recursos novos e aprimorados

Configuração Completa: Suporte para provisionamento de VMs AWS e GCP usando perfis de máquina. Ao provisionar VMs AWS ou GCP usando o Machine Creation Services (MCS), agora você pode selecionar uma VM existente como perfil de máquina, permitindo que as VMs dentro do catálogo herdem as configurações da VM selecionada.

- Para VMs GCP, as configurações herdadas incluem ID do Conjunto de Criptografia de Disco, Tamanho da máquina, Tipo de armazenamento e Zona.
- Para VMs AWS, as configurações herdadas variam com base no estágio:
  - Durante a criação do catálogo: Tamanho da máquina, Tipo de locação, Grupo de segurança e o número de NICs.
  - Durante a edição do catálogo: Tamanho da máquina e Grupo de segurança.

Para obter mais informações, consulte Criar um catálogo de máquinas.

Introdução da funcionalidade de pesquisa nos nós Catálogos de Máquinas e Grupos de Entrega. Agora você pode pesquisar e localizar diretamente catálogos de máquinas e grupos de entrega dentro dos nós **Catálogos de Máquinas** e **Grupos de Entrega**. A funcionalidade de pesquisa nesses nós oferece a mesma interface que o nó **Pesquisar**, proporcionando uma experiência de pesquisa contínua em todo o DaaS. Para obter mais informações, consulte Usar Pesquisa na interface de gerenciamento de Configuração Completa.

Visualizar o status do dispositivo de endpoint em Diagnóstico de Inicialização de Sessão usando o Device Posture. O recurso Diagnóstico de Inicialização de Sessão no Monitor ajuda a identificar o componente e o estágio exatos onde ocorreu uma falha de sessão. Isso ajuda a identificar a razão exata para uma falha de inicialização de sessão e a tomar a ação recomendada.

Como próximo passo para tornar essa verificação abrangente em todos os componentes envolvidos na sequência de inicialização da sessão, agora você pode visualizar os resultados da varredura do dispositivo de endpoint. Clicar em **Dispositivo de Endpoint** na lista de componentes mostra o status da varredura do Device Posture. O Serviço Device Posture verifica o dispositivo de endpoint quanto à conformidade com base nas políticas definidas pelo administrador.

Certifique-se de que o serviço Device Posture esteja configurado com o DaaS conforme descrito no artigo Device Posture. Os erros registrados pelo Device Posture são descritos em Logs de Erro do Device Posture.

Para obter mais informações, consulte Etapas para diagnosticar falha no lançamento da sessão

Novas opções na Configuração Completa para rotear solicitações de API para Azure e GCP através dos Citrix Cloud Connectors. Anteriormente, as solicitações de API para Azure e GCP podiam ser roteadas apenas através de endpoints públicos. Com uma nova opção em **Configuração Completa > Adicionar Conexão e Recursos**, agora você pode optar por uma

abordagem mais segura, roteando-as através dos Citrix Cloud Connectors. Para obter mais informações, consulte Criar um principal de serviço e conexão usando a Configuração Completa.

Aprimoramentos de pesquisa e filtro. Fizemos os seguintes aprimoramentos para melhorar sua experiência de pesquisa:

- **Pesquisa simplificada**: Realizar uma pesquisa sem filtros agora remove as recomendações de pesquisa, proporcionando uma experiência de pesquisa limpa e direta.
- **Atualização do operador E/OU**: As opções "Corresponder a todos (operador E)" e "Corresponder a qualquer (operador OU)" agora estão disponíveis no painel de filtros, acessíveis com um único clique no ícone de filtros.
- **Configuração de filtro simplificada**: Agora você pode especificar e aplicar vários filtros de forma contínua com o painel de filtros.
- **Interface mais limpa**: A capacidade de "fixar filtro" foi removida, reduzindo a desordem da interface do usuário e tornando sua experiência de pesquisa mais intuitiva.
- **Adição rápida de filtro**: Após aplicar filtros, agora você pode usar o sinal de mais para adicionar rapidamente mais um filtro.
- **Excluir conjuntos de filtros salvos**: Agora você pode excluir facilmente conjuntos de filtros salvos diretamente no menu de pesquisa, sem precisar navegar até **Gerenciar conjuntos de filtros**.

Para obter mais informações, consulte Usar Pesquisa na interface de gerenciamento de Configuração Completa.

Suporte à atualização de VDA para catálogos de máquinas criados com o Azure Quick Deploy. Com a Configuração Completa, agora você pode habilitar a **Atualização de VDA** para catálogos de máquinas criados através do Azure Quick Deploy e, em seguida, executar a **Atualização de VDA** neles para atualizações imediatas ou agendadas. Para obter mais informações, consulte Atualizar VDAs usando a interface de Configuração Completa.

Capacidade de redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado por MCS no SCVMM. Agora você pode usar o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado por MCS. O recurso automatiza o processo de redefinição do disco do SO. Por exemplo, ele ajuda a redefinir a VM para seu status inicial de um catálogo de desktop de desenvolvimento persistente criado usando MCS. Atualmente, esse recurso é aplicável a ambientes de virtualização Azure, Citrix Hypervisor, SCVMM e VMware. Para obter mais informações sobre como usar o comando PowerShell para redefinir o disco do SO, consulte Redefinir disco do SO.

Atualizar propriedades de VMs individuais. Agora você pode atualizar as propriedades de VMs individuais em um catálogo de máquinas MCS persistente usando um comando PowerShell. Essa implementação ajuda você a gerenciar VMs individuais de forma eficiente sem atualizar todo o catálogo de máquinas. Atualmente, esse recurso é aplicável apenas ao ambiente Azure. Para obter mais informações, consulte Atualizar propriedades de VMs individuais.

Restringir upload e download de discos gerenciados. De acordo com a política do Azure, você não pode fazer upload ou download de mais de cinco discos ou snapshots ao mesmo tempo com o mesmo objeto de acesso ao disco. Com esse recurso, o limite de cinco uploads ou downloads simultâneos não é imposto se você:

- Configure `ProxyHypervisorTrafficThroughConnector` em `CustomProperties`, e
- Não configure a política do Azure para criar Acessos de Disco automaticamente para cada novo disco usar endpoints privados.

Suporte para atribuir uma letra de unidade específica ao disco de cache de write-back de E/S do MCS. Anteriormente, o sistema operacional Windows atribuía automaticamente uma letra de unidade ao disco de cache de write-back de E/S do MCS. Com esse recurso, agora você pode atribuir uma letra de unidade específica a um disco de cache de write-back de E/S do MCS. Essa implementação ajuda a evitar conflitos entre a letra de unidade de quaisquer aplicativos que você usa e a letra de unidade do disco de cache de write-back de E/S do MCS. Esse recurso é aplicável apenas ao sistema operacional Windows. Para obter mais informações, consulte Atribuir uma letra de unidade específica ao disco de cache de write-back de E/S do MCS.

Suporte para perfil de máquina no Citrix Hypervisor. No Citrix Hypervisor, agora você pode criar um catálogo de máquinas MCS usando um perfil de máquina. A origem da entrada do perfil de máquina é uma VM. O perfil de máquina captura as propriedades de hardware de um modelo de VM e as aplica às VMs recém-provisionadas no catálogo. Para obter mais informações, consulte Criar um catálogo de máquinas usando um perfil de máquina.

Tentar novamente a criação do catálogo após falha. Quando a criação do catálogo falha, agora você pode tentar novamente criar o catálogo. Para garantir a criação bem-sucedida, verifique as informações de solução de problemas e resolva os problemas. As informações descrevem os problemas encontrados e fornecem recomendações para resolvê-los. Os catálogos com falha são marcados com um ícone de erro. Para ver os detalhes, vá para a guia **Solução de problemas** de cada catálogo. Para obter mais informações, consulte Gerenciar catálogos de máquinas.

Permissão para gerenciar conjuntos de configuração. Para permitir um controle mais preciso sobre o gerenciamento de conjuntos de configuração do WEM, introduzimos uma nova permissão chamada **Gerenciar conjuntos de configuração** ao conjunto de permissões **Catálogos de**

máquinas. Essa permissão concede acesso exclusivo a usuários que podem executar tarefas como vincular ou desvincular um conjunto de configuração e alternar para um conjunto de configuração diferente para catálogos. Para obter mais informações, consulte Gerenciar conjunto de configuração para um catálogo.

Nova opção na Configuração Completa para habilitar a limpeza de dispositivos obsoletos ingressados no Azure AD. Introduzimos uma opção na Configuração Completa para simplificar a limpeza de dispositivos obsoletos ingressados no Azure AD no Citrix DaaS. Anteriormente, você precisava executar um script PowerShell personalizado para realizar a tarefa. Habilitar essa opção concede permissão às conexões de host para limpar automaticamente dispositivos obsoletos ingressados no Azure AD. Para obter mais informações, consulte Conexões de host do Azure.

Monitorar o status de atualização da imagem para catálogos usando a Configuração Completa. Agora você pode monitorar os status de atualização da imagem para catálogos de máquinas não persistentes usando uma nova coluna, **Atualização da Imagem**. Esta coluna indica se as imagens de um catálogo estão **Totalmente atualizadas**, **Parcialmente atualizadas** ou **Atualização pendente**.

Para mostrar a coluna na tabela **Catálogos de Máquinas**, siga estas etapas:

1. No nó **Catálogos de Máquinas**, selecione o ícone **Colunas a Exibir** na barra de ações.
2. Selecione **Catálogo de Máquinas > Status da Imagem**.
3. Clique em **Salvar**.

Exibir a coluna **Atualização da imagem** pode degradar o desempenho do console. Recomendamos exibi-la apenas quando necessário.

Ambiente seguro para tráfego gerenciado pelo GCP. Com esse recurso, agora você pode permitir apenas acesso privado do Google aos seus projetos do Google Cloud. Essa implementação aprimora a segurança para manipular dados confidenciais. Para fazer isso, adicione `ProxyHypervisorTrafficThroughConnector` em `CustomProperties` no caso de implantação do Citrix Cloud. Se você estiver usando um pool de trabalhadores privado, adicione `UsePrivateWorkerPool` em `CustomProperties`. Para obter mais informações, consulte Criar um ambiente seguro para tráfego gerenciado pelo GCP.

Julho de 2023

Recursos novos e aprimorados

Suporte para obter uma lista de recursos órfãos no Azure. Em ambientes Azure, agora você pode obter uma lista de recursos órfãos que são criados pelo MCS, mas não são mais usados pelo MCS. Esse recurso ajuda a evitar custos extras. Para obter mais informações, consulte Recuperar uma lista de recursos órfãos.

Suporte para a criação de máquinas persistentes de várias sessões usando a Configuração Completa. Ao criar um catálogo de máquinas de várias sessões, agora você pode especificar se elas devem ser persistentes. Para máquinas persistentes de várias sessões, lembre-se de que as alterações que os usuários fazem nos desktops são salvas e acessíveis a todos os usuários autorizados. Para obter mais informações, consulte Criar catálogos de máquinas.

Nova capacidade na Configuração Completa para filtrar o inventário de AMI da AWS. Ao selecionar modelos de máquina durante a criação do catálogo da AWS, agora você pode filtrar o inventário de AMI da AWS para um modelo de destino usando estes critérios de pesquisa:

- Nome da imagem
- ID da imagem
- Tags da imagem

A lista de modelos de máquina é carregada dinamicamente à medida que você rola a lista para baixo — 25 itens são carregados inicialmente e mais são carregados à medida que você rola.

Suporte para exclusão de dispositivos Azure AD. Com esse recurso, dispositivos Azure AD obsoletos podem ser excluídos de forma consistente, atribuindo a função de Administrador de Dispositivos na Nuvem ao principal de serviço e modificando a propriedade personalizada da conexão de hospedagem. Se você não excluir os dispositivos AD obsoletos do Azure, a VM não persistente correspondente permanecerá no estado de inicialização até que você a remova manualmente do portal do Azure AD. Para obter mais informações, consulte Pool de identidades de identidade de máquina unida ao Azure Active Directory.

Suporte para perfil de máquina em ambiente AWS. Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS) na AWS, agora você pode usar um perfil de máquina para capturar as propriedades de hardware de uma instância EC2 (VM) ou versão de modelo de inicialização e aplicá-las às máquinas provisionadas. As propriedades capturadas podem incluir, por exemplo, propriedades de volume EBS, tipo de instância, otimização EBS e outras configurações AWS suportadas. Ao editar o catálogo, o perfil da máquina das máquinas

provisionadas pode ser alterado fornecendo uma VM ou modelo de inicialização diferente. Para obter mais informações, consulte Criar um catálogo usando um perfil de máquina.

Limite de exportação de resultados de pesquisa estendido para 30.000 de 10.000. Estendemos o limite de exportação de resultados de pesquisa. Anteriormente restrito a 10.000 itens, agora você pode exportar até 30.000 itens para um arquivo CSV. Para obter mais informações, consulte Exportar resultados de pesquisa para um arquivo CSV.

Opção de atualização de imagem. Ao selecionar imagens mestre para catálogos de máquinas, agora você pode obter rapidamente a lista de imagens mestre mais atualizada usando a opção **Atualizar** no canto superior direito. Observe que a opção **Atualizar** não está disponível para catálogos AWS. Além disso, uma opção **Atualizar** está disponível para perfis de máquina e grupos de host em catálogos do Azure.

Junho de 2023

Recursos novos e aprimorados

Suporte para obter propriedades personalizadas da entrada do perfil da máquina no GCP. Anteriormente, em ambientes GCP, ao criar um catálogo de máquinas MCS usando uma entrada de perfil de máquina, você tinha que especificar explicitamente as propriedades personalizadas. A ação exigia um esforço extra. Com esse recurso, agora você pode derivar as seguintes propriedades personalizadas sem defini-las explicitamente:

- `ServiceOffering`
- `CryptoKeyId`
- `CatalogZones`
- `Storage`

Ao executar os comandos `New-ProvScheme` e `Set-ProvScheme` e não especificar explicitamente as propriedades personalizadas, os valores das propriedades são derivados da entrada do perfil da máquina.

Por exemplo, `New-ProvScheme -MachineProfile` grava o tipo de máquina do perfil da máquina na propriedade `ServiceOffering` do esquema de provisionamento, a menos que você especifique `ServiceOffering` no comando `New-ProvScheme`. Se você executar `Set-ProvVMScheme` duas vezes, o comando mais recente terá efeito.

Remover tags em ambientes AWS. Anteriormente, os comandos PowerShell `Remove-ProvVM` e `Remove-ProvScheme` com o parâmetro `ForgetVM` removiam as VMs e os catálogos de máquinas do banco de dados Citrix. No entanto, os comandos não removiam as tags. Você tinha que gerenciar individualmente as VMs e os catálogos de máquinas que não eram removidos completamente de todos os recursos. Com este recurso, você pode usar:

- `Remove-ProvVM` com o parâmetro `ForgetVM` para remover VMs e tags de uma única VM ou de uma lista de VMs de um catálogo de máquinas.
- `Remove-ProvScheme` com o parâmetro `ForgetVM` para remover um catálogo de máquinas do banco de dados Citrix e recursos de um catálogo de máquinas.

Esta implementação ajuda em:

- Identificar recursos vazados
- Remover o custo adicional de manutenção dos recursos que não são necessários

Este recurso é aplicável apenas a VMs persistentes. Para obter mais informações, consulte Remover tags.

Capacidade de obter erros e avisos históricos associados a um catálogo de máquinas MCS. Anteriormente, você só obtinha os avisos e erros mais recentes associados a um catálogo de máquinas. Com este recurso, agora você pode obter uma lista dos avisos e erros históricos de um catálogo de máquinas MCS. Esta lista ajuda você a entender quaisquer problemas com seu catálogo de máquinas MCS e a corrigi-los.

Para obter mais informações, consulte Recuperar avisos e erros associados a um catálogo.

Capacidade aumentada com desempenho aprimorado para Citrix no Google Cloud. O Citrix agora pode suportar catálogos contendo até 3.000 VDAs em um único projeto do Google Cloud. Esta atualização traz melhorias de desempenho para as operações de provisionamento e gerenciamento de energia.

Capacidade de redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado por MCS em ambientes Google Cloud e AWS. Agora você pode usar o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado por MCS. O recurso automatiza o processo de redefinição do disco do SO. Por exemplo, ele ajuda a redefinir a VM para seu status inicial de um catálogo de desktop de desenvolvimento persistente criado usando MCS. Atualmente, este recurso é aplicável a ambientes de virtualização AWS, Azure, Citrix Hypervisor, Google Cloud e VMware. Para obter

mais informações sobre como usar o comando PowerShell para redefinir o disco do SO, consulte Redefinir disco do SO.

Suporte para alteração de propriedades personalizadas relacionadas a disco de um catálogo existente e VMs existentes no GCP. Anteriormente, em ambientes GCP, você podia adicionar as propriedades personalizadas apenas ao criar o catálogo de máquinas MCS. Com este recurso, agora você pode alterar as seguintes propriedades personalizadas relacionadas a disco de um catálogo existente e VMs existentes do catálogo.

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

Esta implementação ajuda você a selecionar diferentes tipos de armazenamento para diferentes discos mesmo após a criação de um catálogo e, assim, equilibrar os preços associados a diferentes tipos de armazenamento. Para obter mais informações, consulte Alterar propriedades personalizadas relacionadas a disco de um catálogo existente.

Suporte a tempo limite de sessão dinâmico estendido para VDA versão 2203 LTSR CU3 ou posterior. Para grupos de entrega de SO de sessão única, este recurso agora se aplica a VDAs da versão 2206 CR ou posterior, ou 2203 LTSR CU3 ou posterior. Para obter mais informações, consulte Tempos limite de sessão dinâmicos.

Experiência aprimorada de criação de conexão de host na Configuração Completa. Depois de selecionar um local de recurso, a lista suspensa **Tipo de conexão** agora exibe todos os hipervisores e serviços de nuvem suportados pelo Citrix, e suas disponibilidades dependem de:

- Para um local de recurso sem Cloud Connectors acessíveis, apenas hipervisores e serviços de nuvem que suportam implantações sem conector estão disponíveis.
- Para um local de recurso com Cloud Connectors acessíveis, apenas hipervisores e serviços de nuvem que têm seus plug-ins instalados corretamente nesses conectores estão disponíveis.

Para obter mais informações, consulte Criar e gerenciar conexões.

Seleção de componentes adicionais na atualização do VDA. Agora você pode selecionar quais componentes adicionais atualizar ou instalar ao atualizar um VDA. Para obter mais informações, consulte atualizar VDAs.

> **Importante:**
>
> Para usar o recurso de componentes adicionais, certifique-se de que seu VDA Upgrade Agent seja a versão 7.34 ou posterior, que está incluída no instalador do VDA versão 2206 ou posterior.

> **A Configuração Completa agora pré-configura determinadas configurações para máquinas Azure com base em perfis de máquina.** Ao provisionar VMs do Azure, a Configuração Completa agora pré-configura as seguintes configurações com base no perfil de máquina selecionado:

- Grupo de host
- Conjunto de Criptografia de Disco
- Zona de Disponibilidade
- Tipo de Licença

Suporte para hibernação de instância AWS. Agora você pode iniciar instâncias AWS, configurá-las conforme desejado e hiberná-las. O processo de hibernação armazena o estado em memória da instância, juntamente com seus endereços IP privados e elásticos, permitindo que ela continue exatamente de onde parou. Para obter mais informações sobre como criar VMs que suportam hibernação, consulte Hibernação de Instância.

Suporte para otimização de limitação de AWS. Agora você pode ligar e desligar um grande número de máquinas em um catálogo AWS sem encontrar problemas de limitação. Problemas de limitação ocorrem quando o número de solicitações enviadas à AWS excede o número de solicitações que o servidor pode manipular. Este recurso aumenta a eficiência ao reduzir o número de chamadas da AWS para ligar e desligar máquinas em massa. Também reduz significativamente o tempo necessário para ligar e desligar máquinas em catálogos persistentes.

Ambiente seguro para tráfego gerenciado do Azure. Anteriormente, você dependia da internet pública para permitir que seus endpoints do Azure interagissem com recursos em seu ambiente. Como resultado, surgiram preocupações de segurança porque a internet pública era acessada. Com este recurso, o MCS permite que o tráfego de rede seja roteado através dos Citrix Cloud Connectors em seu ambiente. Isso torna o ambiente seguro porque agora todo o tráfego gerenciado do Azure se origina do seu próprio ambiente. Para fazer isso, adicione

`ProxyHypervisorTrafficThroughConnector` em `CustomProperties`. Para obter mais informações, consulte Criar um ambiente seguro para tráfego gerenciado do Azure.

Depois de definir as propriedades personalizadas, você pode configurar políticas do Azure para ter acesso privado a discos gerenciados do Azure.

Suporte para provisionamento de VMs de catálogo com o Azure Monitor Agent. O Azure Monitor Agent (AMA) coleta dados de monitoramento e os entrega ao Azure Monitor. Com este recurso, você pode provisionar VMs de catálogo de máquinas MCS (persistentes e não persistentes) com o AMA instalado como uma extensão. Esta implementação permite o monitoramento identificando exclusivamente as VMs nos dados de monitoramento. Para obter mais informações sobre o AMA, consulte Visão geral do Azure Monitor Agent.

Atualmente, o MCS suporta apenas o fluxo de trabalho de perfil de máquina para este recurso. Para obter mais informações sobre o provisionamento de VMs de catálogo de máquinas com o AMA ativado, consulte Provisionar VMs de catálogo com o Azure Monitor Agent instalado.

Habilitar agendamento de reinicialização para um catálogo MCS. Anteriormente, você podia agendar atualizações de imagem esperando pela próxima reinicialização ou acionando uma reinicialização imediata de todas as VMs. Com este recurso, agora você pode criar um agendamento de reinicialização única para um catálogo, a ser acionado em uma data e hora desejadas para facilitar as atualizações de imagem do MCS. Para criar um agendamento de reinicialização, use o comando `BrokerCatalogRebootSchedule`. Para obter mais informações, consulte Alterar a imagem mestre.

Gerenciar segredos de cliente expirados no Azure Quick Deploy. No Azure Quick Deploy, agora você pode se manter informado com alertas quando os segredos do cliente expiram e atualizá-los facilmente para garantir o acesso contínuo aos recursos do Azure. Para obter mais informações, consulte Atualizar segredos de cliente expirados.

Maio de 2023

Recursos novos e aprimorados

Aprimoramentos na pesquisa. Este recurso aprimora os visuais e as interações para filtros, proporcionando uma melhor experiência de pesquisa. Para obter mais informações, consulte Usar a pesquisa na interface de gerenciamento de Configuração Completa.

Nova política de exclusões de usuário onde você pode definir caminhos de diretório que não são redirecionados para a camada de usuário. As exclusões de usuário se aplicam à camada de personalização do usuário (UPL), mas não ao host da sessão. O Logoff.txt agora

contém todas as exclusões de usuário ativas. Para obter mais informações, consulte Camada de personalização do usuário.

Suporte para atualização da versão de hardware de novas VMs adicionadas em um catálogo de máquinas MCS. Em ambientes VMware, agora você pode atualizar a versão de hardware das VMs recém-adicionadas em um catálogo de máquinas MCS existente usando uma fonte de perfil de máquina. Você não precisa criar um novo catálogo de máquinas para atualizar a versão de hardware das VMs adicionadas a um catálogo. Você deve usar o fluxo de trabalho de perfil de máquina para usar este recurso.

Suporte para filtragem de instâncias de VM AWS. Anteriormente, ao usar uma instância de VM AWS como entrada de perfil de máquina para criar um catálogo de máquinas MCS, o catálogo às vezes não era criado ou não funcionava corretamente devido a uma entrada de perfil de máquina inválida. Com este recurso, agora você pode listar as instâncias de VM AWS que podem ser usadas como VMs de perfil de máquina válidas. Para fazer isso, use o comando `Get-HypInventoryItem`. Para obter mais informações, consulte Filtragem de instâncias de VM.

Suporte para a conversão de catálogos de máquinas: de não baseados em perfil para baseados em perfil no ambiente Azure. No ambiente Azure, agora você pode usar uma VM ou uma especificação de modelo como entrada de perfil de máquina para converter um catálogo de máquinas que não é baseado em perfil de máquina em um que o seja. As VMs existentes e as novas VMs adicionadas ao catálogo herdam os valores de propriedade do perfil de máquina, a menos que sejam substituídos por propriedades personalizadas explícitas. Para obter mais informações, consulte Converter um catálogo de máquinas não baseado em perfil de máquina em um que o seja.

Suporte para criptografia dupla em disco gerenciado no ambiente Azure. No ambiente Azure, agora você pode criar um catálogo de máquinas MCS com criptografia dupla. A criptografia dupla é a criptografia do lado da plataforma (padrão) e a criptografia gerenciada pelo cliente (CMEK). Portanto, se você é um cliente altamente sensível à segurança que está preocupado com o risco associado a qualquer algoritmo de criptografia, implementação ou uma chave comprometida, você pode optar por esta criptografia dupla. Discos de SO e dados persistentes, instantâneos e imagens são todos criptografados em repouso com criptografia dupla. Para obter mais informações, consulte Criptografia dupla em disco gerenciado.

Suporte para perfil de máquina no VMware. Em ambientes VMware, agora você pode criar um catálogo de máquinas MCS usando um perfil de máquina. A fonte da entrada do perfil de máquina é um modelo VMware. O perfil de máquina captura as propriedades de hardware de um modelo

VMware e as aplica às VMs recém-provisionadas no catálogo. Para obter mais informações, consulte Criar um catálogo de máquinas usando um perfil de máquina.

Capacidade de redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado por MCS no Azure e Citrix Hypervisor. Agora você pode usar o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado por MCS. O recurso automatiza o processo de redefinição do disco do SO. Por exemplo, ele ajuda a redefinir a VM para seu status inicial de um catálogo de desktop de desenvolvimento persistente criado usando MCS. Atualmente, este recurso é aplicável a ambientes de virtualização Azure, Citrix Hypervisor e VMware. Para obter mais informações sobre como usar o comando PowerShell para redefinir o disco do SO, consulte Redefinir disco do SO.

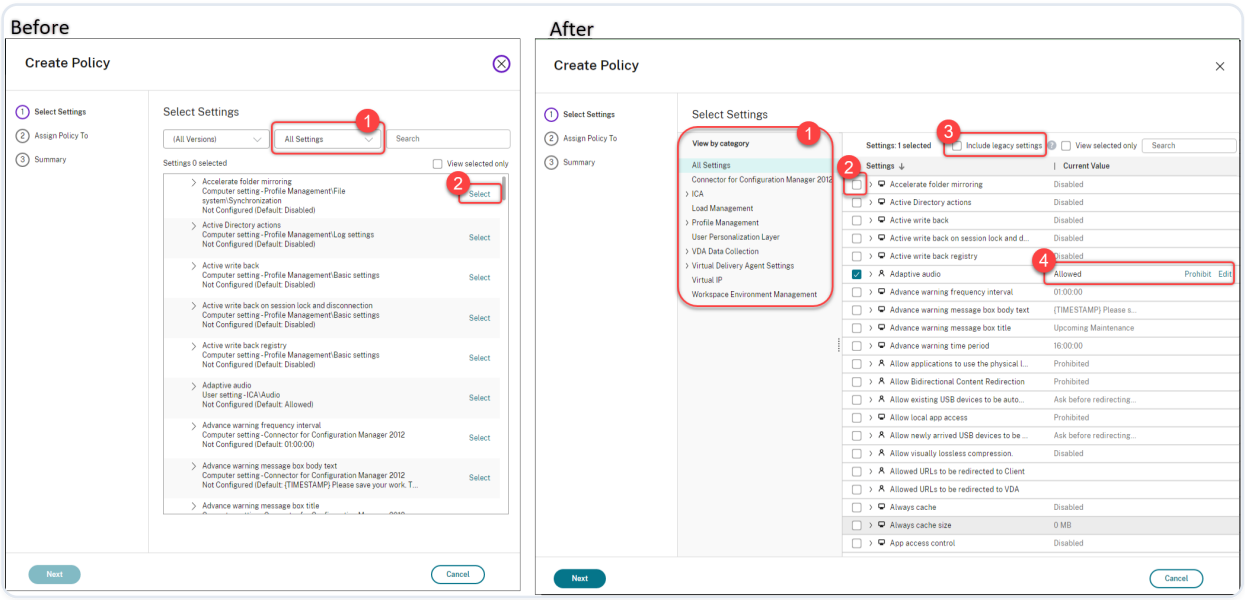
Experiência aprimorada de criação de conexão de host. Agora você pode obter as seguintes informações ao criar uma conexão de host:

- Lista de todos os plug-ins de hipervisor suportados pela Citrix, incluindo plug-ins de terceiros
- Disponibilidade do plug-in do hipervisor. Se o status de disponibilidade for falso, o motivo possível pode ser que o Cloud Connector não esteja instalado

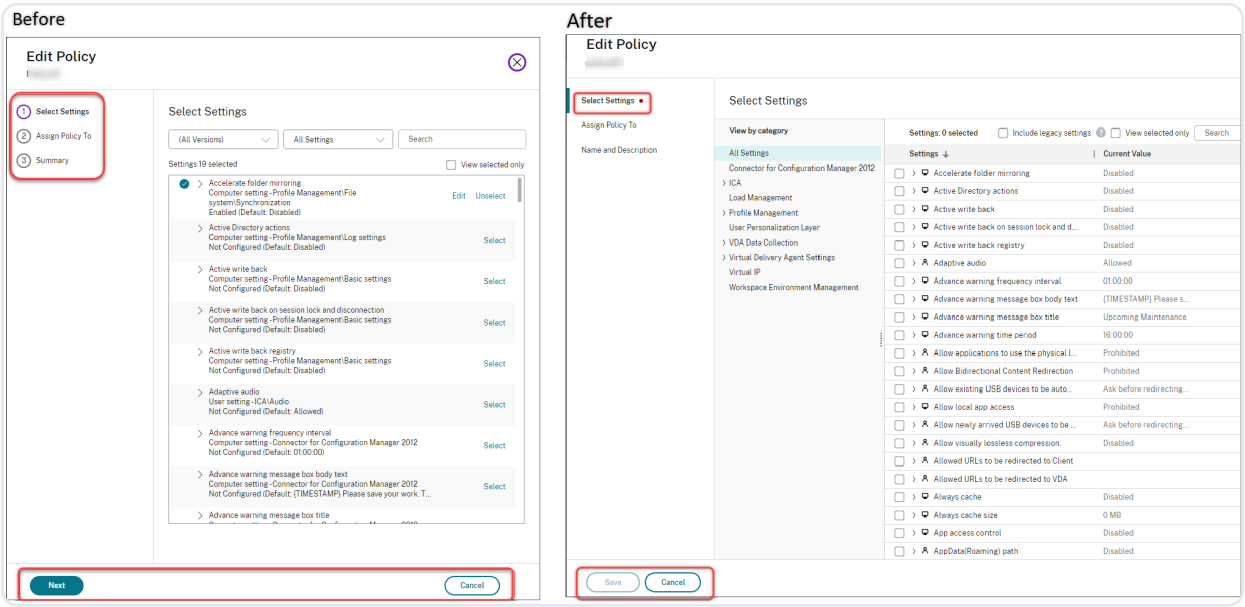
Este recurso ajuda você a configurar corretamente um local de recurso e, assim, criar uma conexão de host. Para obter mais informações, consulte Etapa 1. Conexão.

Melhorias na experiência do usuário para o nó Políticas. Para melhorar a experiência do usuário e tornar o gerenciamento de políticas mais eficiente, implementamos as seguintes melhorias no nó **Configuração Completa > Políticas**:

- Novo design da interface do usuário para as ações **Criar Política** e **Criar Modelo**:
  - Visualização de pasta expansível para configurações de política. Na página **Selecionar Configurações**, todas as configurações são exibidas por categoria em uma visualização de árvore expansível, facilitando a localização de uma configuração.
  - Para selecionar uma configuração, basta clicar em uma caixa de seleção em vez de usar o botão **Selecionar**.
  - As configurações herdadas foram ocultadas por padrão para que apenas as configurações mais relevantes sejam exibidas. Se as configurações herdadas forem necessárias, selecione **Incluir configurações herdadas**.
  - Um botão de ação foi adicionado ao lado de uma configuração Booleana, permitindo que você altere seu valor diretamente na lista de configurações.



- Novo design da interface do usuário para a ação **Editar Política**:
  - O menu de navegação foi atualizado para uma lista não ordenada. Cada item na lista agora inclui um botão **Salvar** em sua página. Com este novo design, você pode salvar as alterações feitas em um item sem precisar navegar por todos os itens no menu de navegação. Essas melhorias tornam o gerenciamento de políticas mais eficiente e simplificado.
  - Pontos vermelhos aparecem ao lado dos itens de navegação para indicar erros de configuração.



- Arraste para repriorizar políticas. Na lista de prioridades, agora você pode alterar a prioridade de uma política arrastando-a para a posição desejada.

Nova opção para desativar o logoff forçado de usuários para o AutoScale. Uma nova opção, **Não notificar nem forçar o logoff do usuário**, agora está disponível na página **Gerenciar Autoscale > Notificação de Logoff do Usuário**. Com a opção selecionada, o Autoscale não forçará os usuários a fazer logoff de máquinas em estado de drenagem nem notificará os usuários para fazer logoff e logon em uma máquina diferente. Para obter mais informações, consulte Notificações de logoff do usuário.

Capacidade de reiniciar PCs em nuvem do Windows 365. Agora você pode usar o Citrix DaaS para reiniciar PCs em nuvem do Windows 365.

Mais detalhes da sessão. Ao visualizar uma sessão em **Configuração Completa > Pesquisar > Sessões**, a visualização da sessão (no painel inferior) agora inclui mais detalhes da sessão para ajudar você a solucionar problemas e identificar problemas do cliente:

- **Tempo de reconexão.** O tempo em que uma sessão foi reconectada após ser desconectada.
- **Plataforma do cliente.** A plataforma usada para iniciar a sessão.
- **Versão do cliente.** A versão da plataforma do cliente usada para iniciar a sessão.
- **IP do host remoto.** O endereço IP do host remoto onde o Citrix Workspace está sendo hospedado.

Suporte para renomear grupos de segurança do Azure AD para VMs. Para VMs adicionadas a um grupo de segurança do Azure AD através do Citrix DaaS, agora você pode renomear o grupo de segurança usando **Configuração Completa > Editar Catálogo de Máquinas**. A renomeação ocorre depois que você salva a alteração.

Seleção de domínio padrão para contas de máquina. Ao criar um catálogo, o domínio onde o recurso (conexão) reside é selecionado por padrão para contas de máquina.

Capacidade de exibir os grupos de segurança atribuídos do Azure AD para VMs ingressarem. Na Configuração Completa, ao criar VMs ingressadas no Azure Active Directory, uma opção, **Ingressar em um grupo de segurança atribuído como membro**, agora está disponível, permitindo que você adicione o grupo de segurança do Azure AD onde as VMs residem a um grupo de segurança atribuído. Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Suporte para alterar redes para conexões. Na Configuração Completa, agora você pode alterar as redes para uma conexão. Você não pode desassociar redes de uma conexão se elas estiverem em uso. Para obter mais informações, consulte Editar rede.

Capacidade de remover tags em ambientes Azure. Anteriormente, os comandos PowerShell `Remove-ProvVM` e `Remove-ProvScheme` com o parâmetro `ForgetVM` removiam as VMs e os catálogos de máquinas do banco de dados Citrix. No entanto, os comandos não removiam as tags dos recursos. Você tinha que gerenciar individualmente as VMs e os catálogos de máquinas que não foram totalmente excluídos de todos os recursos. Com este recurso, você pode usar:

- `Remove-ProvVM` com o parâmetro `ForgetVM` para remover VMs e tags criadas nos recursos de uma única VM ou de uma lista de VMs de um catálogo de máquinas.
- `Remove-ProvScheme` com o parâmetro `ForgetVM` para remover um catálogo de máquinas do banco de dados Citrix e tags criadas nos recursos de um catálogo de máquinas inteiro.

Esta implementação ajuda a identificar recursos órfãos que são criados pelo MCS, mas não são mais usados pelo MCS.

Este recurso é aplicável apenas a VMs persistentes. Para obter mais informações, consulte Remover tags.

Alerta de Máquinas com Falha. O recurso de Notificação e Alerta Proativo do Monitor foi aprimorado para incluir um novo alerta, Máquinas com Falha (em %), baseado na porcentagem de máquinas com falha em um grupo de entrega. A nova condição de alerta permite configurar limites de alerta como uma porcentagem de máquinas com falha em um grupo de entrega. Para obter mais informações, consulte a seção Máquinas com Falha no artigo Alertas.

Abril de 2023

Recursos novos e aprimorados

Publicação com plataformas de nuvem específicas usando Citrix Provisioning no Image Portability Service. Fluxos de trabalho específicos para usar o Image Portability Service para publicar no AWS, Azure e Google Cloud estão agora disponíveis. Além disso, as permissões necessárias para Azure e rede foram atualizadas. Para mais detalhes, consulte Migrar cargas de trabalho para a nuvem pública.

Suporte para identificar por que uma máquina está em modo de manutenção. Anteriormente, o PowerShell era sua única opção para identificar por que uma máquina estava em modo de manutenção. Agora você pode fazer isso na Configuração Completa:

1. Use Pesquisar para localizar a máquina.
2. Verifique **Motivo da Manutenção** na guia **Detalhes** no painel inferior. Ou passe o mouse sobre a coluna **Modo de Manutenção**. As seguintes informações podem aparecer:

- Pelo Administrador: Colocado em modo de manutenção pelo administrador.
- Máximo de Registros Falhos: Colocado em modo de manutenção porque a máquina excedeu o número máximo de tentativas de registro permitidas.

Além disso, um filtro, **Motivo da Manutenção**, está agora disponível. Você pode usá-lo para identificar as máquinas de destino.

O recurso é útil para administradores solucionarem problemas com máquinas em modo de manutenção.

Use variáveis para notificar os usuários sobre o tempo restante antes de serem desconectados. Ao forçar o logoff do usuário, agora você pode usar `%s%` ou `%m%` como variáveis para indicar o tempo especificado na mensagem de notificação. Para expressar o tempo em segundos, use `%s%`. Para expressar o tempo em minutos, use `%m%`. Para mais informações, consulte Notificações de logoff do usuário.

Suporte para personalizar o comportamento de inicialização em caso de falha na alteração do tipo de armazenamento. Ao ligar, o tipo de armazenamento de um disco gerenciado pode falhar ao mudar para o tipo desejado devido a uma falha no Azure. Anteriormente, nesses cenários, a VM permaneceria desligada com uma mensagem de falha enviada a você. Com este recurso, você pode optar por ligar a VM mesmo quando o armazenamento não puder ser restaurado para o tipo configurado ou optar por manter a VM desligada. Para mais informações, consulte Personalizar o comportamento de inicialização em caso de falha na alteração do tipo de armazenamento.

Suporte para ativação MAK. Agora você pode provisionar catálogos de máquinas persistentes e não persistentes com VMs ativadas através da Chave de Ativação Múltipla (MAK). Com este recurso, agora o MCS também pode se comunicar com VMs provisionadas. Esta implementação ajuda a ativar o sistema Windows sem perder as contagens de ativação. Para mais informações, consulte Ativação de licenciamento por volume.

Suporte para criptografia de disco do Azure no host. Com este recurso, agora você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host. Atualmente, o MCS suporta apenas o fluxo de trabalho de perfil de máquina para este recurso. Você pode usar uma VM ou uma especificação de modelo como entrada para um perfil de máquina. Para mais informações, consulte Criptografia de disco do Azure no host.

Nesse tipo de criptografia, o servidor que hospeda a VM criptografa os dados e, em seguida, os dados criptografados fluem através do servidor de armazenamento do Azure. Portanto, este

método de criptografia criptografa os dados de ponta a ponta. Para mais informações, consulte Criptografia no host - Criptografia de ponta a ponta para seus dados de VM.

Suporte para modelo de instância GCP como entrada para perfil de máquina. Com este recurso, agora você pode selecionar um modelo de instância GCP como entrada para o perfil de máquina. Os modelos de instância são recursos leves no GCP, portanto, são muito econômicos. Para fazer isso, use comandos PowerShell. Para mais informações sobre como usar comandos PowerShell para criar e atualizar catálogos de máquinas selecionando um modelo de instância GCP, consulte Criar um catálogo de máquinas com perfil de máquina como um modelo de instância.

Suporte para modificar o nome do grupo de segurança dinâmico do Azure AD. Você pode modificar ou excluir um nome de grupo de segurança dinâmico do Azure AD no portal do Azure. Essa ação pode fazer com que o nome do grupo de segurança dinâmico do Azure AD fique dessincronizado com o grupo de segurança dinâmico associado a um catálogo de máquinas. Com este recurso, agora você pode modificar o nome do grupo de segurança dinâmico do Azure AD associado a um catálogo de máquinas.

Esta modificação ajuda você a tornar as informações do grupo de segurança dinâmico do Azure AD armazenadas no objeto do pool de identidades do Azure AD consistentes com as informações armazenadas no portal do Azure. Para obter mais informações, consulte Modificar o nome do grupo de segurança dinâmico do Azure AD.

Permissões adicionadas necessárias no GCP. As permissões necessárias para fazer o seguinte foram adicionadas:

- Criar conexão de host
- Fazer gerenciamento de energia de VMs
- Provisionar catálogos

Para obter mais informações, consulte Sobre as permissões do GCP.

Tratamento de credenciais. Para maior segurança, por padrão, as credenciais não são encaminhadas para a nuvem para usuários que não estão no mesmo domínio que seus VDAs. As tentativas de login falham quando todas as seguintes condições são atendidas:

- O usuário está em um domínio diferente do VDA
- Nenhuma confiança existe entre os domínios
- O StoreFront está instalado no mesmo domínio que o VDA

Anteriormente, nessas condições, o usuário não podia ser autenticado no StoreFront. Assim, o Cloud Connector encaminhava as credenciais do usuário para a nuvem para rotear a solicitação de autenticação para o destino correto para aquele usuário. Esse comportamento ainda pode ser configurado, se necessário. Para obter mais informações, consulte o parâmetro `CredentialForwardingToCloudAllowed` de Set-Brokersite no SDK do PowerShell do DaaS.

Março de 2023

Recursos novos e aprimorados

Suporte para configurar função e escopo para administradores. O Citrix Cloud agora oferece um maior grau de flexibilidade e personalização ao configurar o acesso para um administrador. Anteriormente, você só podia selecionar pares predefinidos de funções e escopos. Com este aprimoramento, você pode selecionar uma função e, em seguida, emparelhá-la com o escopo de sua escolha.

Para obter mais informações, consulte Configurar acesso personalizado para um administrador.

Suporte para criar grupo de segurança dinâmico em um grupo de segurança atribuído existente. Anteriormente, você podia criar grupos de segurança dinâmicos do Azure AD para um catálogo de máquinas. Com este recurso, você também pode adicionar um grupo de segurança dinâmico do Azure AD em um grupo de segurança atribuído do Azure AD existente. Você pode fazer o seguinte:

- Obter informações do grupo de segurança.
- Obter todos os grupos de segurança atribuídos do Azure AD que são sincronizados de um servidor AD local ou os grupos de segurança atribuídos aos quais as funções do Azure AD podem ser atribuídas.
- Obter todos os grupos de segurança dinâmicos do Azure AD.
- Adicionar grupo de segurança dinâmico do Azure AD como membro de um grupo atribuído do Azure AD.
- Remover a associação entre o grupo de segurança dinâmico do Azure AD e o grupo de segurança atribuído do Azure AD quando o grupo de segurança dinâmico do Azure AD for excluído junto com o catálogo de máquinas.

Para obter mais informações, consulte Criar um grupo de segurança dinâmico do Azure AD em um grupo de segurança atribuído do Azure AD existente.

Suporte para grupo de segurança dinâmico do Azure AD para VM ingressada no Azure AD. A Citrix agora oferece suporte a grupos de segurança dinâmicos para um catálogo ao criar um catálogo de máquinas MCS. As regras de grupo de segurança dinâmico colocam as VMs no catálogo em um grupo de segurança dinâmico com base no esquema de nomenclatura do catálogo de máquinas. Isso é útil quando você deseja gerenciar as VMs pelo Azure Active Directory (Azure AD). Isso também é útil quando você deseja aplicar políticas de Acesso Condicional ou distribuir aplicativos do Intune filtrando as VMs com o grupo de segurança dinâmico do Azure AD. Ao excluir um catálogo, o grupo de segurança dinâmico também é excluído. Para obter mais informações, consulte Grupo de segurança dinâmico do Azure Active Directory.

Para obter mais informações sobre os requisitos de licença para usar grupos de segurança dinâmicos, consulte o documento da Microsoft Criar ou atualizar um grupo dinâmico no Azure Active Directory.

Suporte para adicionar VMs a grupos de segurança do Azure AD por meio da Configuração Completa. Uma opção, **grupo de segurança do Azure AD**, agora está disponível ao criar VMs ingressadas no Azure AD. A opção permite adicionar as VMs a um grupo de segurança do Azure AD com base em seu esquema de nomenclatura. Para obter mais informações, consulte Criar um catálogo do Microsoft Azure.

Suporte para alterar o tipo de armazenamento de VMs existentes para um nível inferior no desligamento em ambientes Azure. Em ambientes Azure, agora você pode economizar custos de armazenamento alterando o tipo de armazenamento de VMs existentes para um nível inferior quando as VMs são desligadas. Para fazer isso, use a propriedade personalizada StorageTypeAtShutdown. Para obter mais informações, consulte Alterar o tipo de armazenamento de VMs existentes para um nível inferior no desligamento.

Suporte para permitir identificadores de segurança ao criar máquinas virtuais. Anteriormente, ao criar novas máquinas virtuais com a configuração especificada por um esquema de provisionamento, você não podia adicionar um identificador de segurança (`ADAccountSid`) ao comando `NewProvVM`. Com este recurso, agora você pode adicionar o parâmetro `ADAccountSid` para identificar exclusivamente as máquinas ao criar novas máquinas virtuais. Para obter mais informações, consulte Adicionar SIDs ao criar máquinas virtuais.

Capacidade de obter avisos associados a catálogos MCS. Anteriormente, você não recebia nenhuma informação indicando que havia problemas com seu catálogo de máquinas. Com este recurso, agora você pode obter avisos para entender os problemas com seus catálogos MCS e corrigi-los.

Os avisos, ao contrário dos erros, não fazem com que uma tarefa de provisionamento iniciada falhe.

Para obter avisos, use comandos PowerShell. Para obter mais informações, consulte Recuperar avisos associados a um catálogo.

Locatários compartilhados para conexões. Agora você pode adicionar locatários e assinaturas que compartilham a Galeria de Computação do Azure com a assinatura da conexão. Como resultado, ao criar ou atualizar catálogos, você pode selecionar imagens compartilhadas desses locatários e assinaturas. Para obter mais informações, consulte Editar configurações de conexão.

Suporte removido para alteração do tipo de SO para catálogos do Azure. Ao alterar imagens de catálogo, apenas as imagens com o mesmo tipo de SO da imagem em uso são exibidas. Com essa melhoria, o Citrix DaaS não oferece mais suporte à alteração do tipo de SO para catálogos do Azure após a criação do catálogo, como a alteração do tipo de SO do Windows para Linux e vice-versa.

Fevereiro de 2023

Recursos novos e aprimorados

Suporte para compartilhamento de imagens entre diferentes locatários do Azure. Anteriormente, em ambientes Azure, você podia compartilhar imagens apenas com assinaturas compartilhadas usando a Galeria de Computação do Azure. Com esse recurso, agora você pode selecionar uma imagem na Galeria de Computação do Azure que pertence a uma assinatura compartilhada diferente em um locatário diferente para criar e atualizar um catálogo MCS. Para obter mais informações, consulte Compartilhamento de imagens entre locatários do Azure.

Modelagem de políticas. O recurso de modelagem de políticas agora está geralmente disponível. Você pode simular políticas para fins de planejamento e teste. Para obter mais informações, consulte Usar o assistente de modelagem de políticas.

Capacidade de ativar ou desativar recursos de visualização. Em Configuração Completa > Início, como administrador do Citrix Cloud com acesso total, agora você pode ativar ou desativar recursos de visualização sem entrar em contato com a Citrix. Para obter mais informações, consulte Página inicial da interface de Configuração Completa.

Diagnóstico de sessão de pesquisa com nome de usuário. Esse recurso permite o uso do Diagnóstico de Inicialização de Sessão começando com o nome de usuário, caso você não tenha o ID da transação. Esse recurso é particularmente útil para administradores de help desk para triar uma sessão com falha se o usuário final não tiver capturado o ID da transação. Você pode

pesquisar um nome de usuário e selecionar uma sessão para triar em uma lista de sessões com falha que o usuário tentou iniciar nas últimas 48 horas. A página Diagnóstico de Inicialização de Sessão mostra os detalhes da sessão com falha. Ela lista o componente exato e o estágio em que a falha ocorreu. Para obter mais informações, consulte o artigo Diagnóstico de Inicialização de Sessão.

Implante aplicativos web e SaaS seguros com o Secure Private Access. Na guia **Configuração Completa > Aplicativos > Aplicativos**, uma nova opção, **Adicionar Aplicativos Web/SaaS**, agora está disponível na barra de ações. A opção permite implantar aplicativos web e SaaS seguros com o Secure Private Access. O Citrix Secure Private Access oferece uma maneira fácil e flexível para usuários remotos acessarem aplicativos baseados em web, SaaS e cliente-servidor usando uma abordagem Zero-Trust. Ele permite o logon único em aplicativos web e SaaS, juntamente com controles de segurança granulares, como marca d'água e controles de copiar/colar, entre outros recursos de segurança. Com o Citrix Secure Private Access, você pode combinar todos os seus aplicativos virtualizados e não virtualizados em um só lugar e aprimorar a experiência do usuário para seus usuários. Consulte Citrix Secure Private Access.

Filtrar conteúdo de log por uma duração de tempo específica. Uma nova opção, **Personalizado**, agora está disponível na lista de duração de tempo em **Configuração Completa > Registro > Eventos**. Use-a para especificar um período dos eventos para os quais você deseja filtrar sua pesquisa. Para obter mais informações, consulte Registro de configuração.

Atualizações para o Autoscale. Atualizamos a opção **Controlar quando o Autoscale começa a ligar máquinas marcadas** para facilitar o entendimento. A opção controla quando o Autoscale começa a ligar máquinas marcadas com base na porcentagem da capacidade restante de máquinas não marcadas. Quando a porcentagem cai abaixo do limite (padrão, 10%), o Autoscale começa a ligar máquinas marcadas. Quando a porcentagem excede o limite, o Autoscale entra no modo de desligamento. Para obter mais informações, consulte Dimensionamento automático de máquinas marcadas (cloud burst).

Políticas de proteção de aplicativos. Agora você pode habilitar a proteção de aplicativos ao criar ou editar um grupo de entrega. O recurso oferece recursos anti-keylogging e anti-captura de tela para sessões de cliente. Para obter mais informações, consulte Criar grupos de entrega e Gerenciar grupos de entrega.

Utilização de GPU em tempo real disponível para GPUs AMD. Agora você pode ver a Utilização de GPU de GPUs AMD Radeon Instinct MI25 e CPUs AMD EPYC 7V12 (Rome) no Monitor. O Monitor já oferece suporte às GPUs NVIDIA Tesla M60. A Utilização de GPU exibe gráficos com a porcentagem de utilização em tempo real da GPU, da memória da GPU e do

Codificador e Decodificador para solucionar problemas relacionados à GPU em VDAs de SO de sessão única e multi-sessão. Os gráficos de Utilização de GPU AMD estão disponíveis apenas para VDAs executando Windows de 64 bits e Citrix Virtual Apps and Desktops 7 2212 ou posterior. Para obter mais informações, consulte Utilização de GPU.

Suporte para agendamento de atualizações de configuração no Azure. Em ambientes Azure, agora você pode agendar um período para as atualizações de configuração das máquinas provisionadas por MCS existentes usando o comando PowerShell `Schedule-ProvVMUpdate`. Qualquer inicialização ou reinicialização durante o período agendado aplica uma atualização de esquema de provisionamento agendada a uma máquina. Você também pode cancelar a atualização de configuração antes do horário agendado usando `Cancel-ProvVMUpdate`.

Você pode agendar e cancelar a atualização de configuração de:

- Uma única ou múltiplas VMs
- Um catálogo inteiro

Para obter mais informações, consulte Agendar atualizações de configuração.

Suporte para usar imagens prontas para Citrix diretamente do Google Cloud Marketplace. Agora você pode navegar e selecionar imagens oferecidas pela Citrix no Google Cloud Marketplace para criar catálogos MCS. Atualmente, o MCS suporta apenas o fluxo de trabalho de perfil de máquina para este recurso. Para obter mais informações, consulte Google Cloud Marketplace.

Limitar o escopo dos grupos de host na Conexão de Host do SCVMM. Anteriormente, a conexão de host com o SCVMM exigia que o administrador tivesse um único grupo de host de nível superior configurado. Isso implicava que o administrador tinha visibilidade de todos os grupos de host, clusters ou hosts abaixo do único grupo de host de nível superior. Com este recurso, em grandes implantações onde um único SCVMM gerencia vários clusters em diferentes data centers, agora você pode limitar o escopo dos grupos de host dos administradores. Para fazer isso, você pode usar a função de Administrador Delegado no console do Microsoft System Center Virtual Machine Manager (VMM) para selecionar os grupos de host aos quais um administrador deve ter acesso. Para obter mais informações, consulte Instalar e configurar um hipervisor.

Suporte para armazenamento com redundância de zona no Azure. Anteriormente, o MCS oferecia apenas armazenamento com redundância local. Com este recurso, o armazenamento com redundância de zona agora é uma opção no Azure, permitindo que você selecione um tipo de armazenamento dependendo do tipo de redundância que deseja usar. O armazenamento com

redundância de zona replica seu disco gerenciado do Azure em várias zonas de disponibilidade, o que permite que você se recupere de uma falha em uma zona utilizando a redundância em outras. Para obter mais informações, consulte Habilitar armazenamento com redundância de zona.

Janeiro de 2023

Recursos novos e aprimorados

Opção para fazer downgrade do disco de armazenamento para HDD Padrão quando as VMs são desligadas. Uma nova opção, **Habilitar economia de custo de armazenamento**, agora está disponível na página **Configurações de Disco** ao criar ou atualizar catálogos do Azure. A opção economiza custos de armazenamento fazendo o downgrade para HDD Padrão para o disco de armazenamento e o disco de cache de write-back quando a VM é desligada. A VM retorna às suas configurações originais na reinicialização. Para obter mais informações, consulte Criar um catálogo do Microsoft Azure.

Suporte para configurar o roaming de sessão na Configuração Completa. Anteriormente, o PowerShell era sua única opção para configurar o roaming de sessão para aplicativos e desktops. Agora você pode fazer isso na **Configuração Completa**. Para obter mais informações, consulte Gerenciar grupos de entrega.

Algumas ações foram renomeadas para melhor alinhamento com seus significados reais. Renomeamos as seguintes ações em **Configuração Completa > Catálogos de Máquina** e **Configuração Completa > Grupos de Entrega**. Os fluxos de trabalho para executar essas ações permanecem inalterados.

- **Atualizar Máquinas** renomeado para **Alterar Imagem Mestra**
- **Atualização de Reversão de Máquina** renomeado para **Reverter Imagem Mestra**
- **Atualizar Catálogo** renomeado para **Alterar Nível Funcional**
- **Atualizar Grupo de Entrega** renomeado para **Alterar Nível Funcional**
- **Desfazer Upgrade de Catálogo** renomeado para **Desfazer Alteração de Nível Funcional**
- **Desfazer Upgrade de Grupo de Entrega** renomeado para **Desfazer Alteração de Nível Funcional**

Suporte para organizar grupos de aplicativos usando pastas. Agora você pode criar pastas aninhadas para organizar grupos de aplicativos para facilitar o acesso. Para obter mais informações, consulte Organizar grupos de aplicativos usando pastas.

Aprimoramentos de restrição para grupos de entrega. Anteriormente, ao restringir o uso de aplicativos ou desktops para um grupo de entrega, você podia especificar apenas os usuários e grupos de usuários que tinham permissão para usá-los em um grupo de entrega. Agora você também pode adicionar usuários e grupos de usuários que deseja bloquear. Esse aprimoramento é útil quando você adiciona um grupo de usuários a uma lista de permissões e, ao mesmo tempo, deseja bloquear um subconjunto de usuários na lista de permissões. Para obter mais informações, consulte Criar grupos de entrega.

Acesse o Citrix Analytics for Performance™ - Detalhes da Sessão no Monitor. A página Detalhes da Sessão do Citrix Analytics for Performance agora está integrada ao Monitor. Clique em **Exibir Linha do Tempo da Sessão** na página Sessões no Monitor para visualizar a página Detalhes da Sessão do Citrix Analytics for Performance dentro do Monitor. Isso exige que você tenha um direito válido do Citrix Analytics for Performance. Os Detalhes da Sessão estão disponíveis para sessões categorizadas como Excelente, Razoável ou Ruim no Citrix Analytics for Performance.

Você pode visualizar uma tendência da experiência da sessão para a sessão nos últimos três dias, juntamente com os fatores que contribuem para a experiência. Essas informações complementam os dados em tempo real disponíveis no Monitor, usados pelo administrador do helpdesk ao solucionar problemas relacionados à experiência da sessão.

Para obter mais informações, consulte o artigo Site Analytics.

VMs não persistentes são excluídas de hipervisores ou serviços de nuvem quando você as exclui ou seus catálogos de máquinas na Configuração Completa. A opção de reter VMs em hipervisores ou serviços de nuvem agora está disponível apenas para VMs persistentes. Para obter mais informações, consulte Gerenciar catálogos de máquinas.

Dezembro de 2022

Recursos novos e aprimorados

Suporte para a criação de catálogos com associação ao Azure AD (incluindo a híbrida) e habilitados para Microsoft Intune, utilizando VMs mestre associadas ao Azure AD. Agora você pode criar catálogos com associação ao Azure AD (incluindo a híbrida) e habilitados para Microsoft Intune, utilizando VMs mestre que podem ser associadas ao Azure AD (incluindo a híbrida) ou não associadas ao domínio. Se você deseja gerenciar uma VM mestre pelo Microsoft Intune, use a versão 2212 ou posterior do VDA e não ignore a preparação da imagem ao criar ou atualizar catálogos de máquinas.

Para obter mais informações sobre identidades de máquina, consulte Unido ao Azure Active Directory, Microsoft Intune e Unido ao Azure Active Directory Híbrido.

Suporte no MCS para exclusão de objetos de VM sem acessar o hipervisor. Agora você pode excluir objetos de VM no MCS sem ter acesso ao hipervisor. Ao excluir uma VM ou esquema de provisionamento, o MCS precisa remover as tags para que os recursos não sejam mais rastreados ou identificados. Anteriormente, se o hipervisor não pudesse ser acessado, as falhas na remoção de tags eram ignoradas. Com esse recurso, se o hipervisor não estiver acessível ao usar o comando `Remove-ProvVM`, a remoção da tag falhará, mas usando a opção `PurgeDBOnly`, você ainda poderá excluir o objeto de recurso da VM do banco de dados. Para obter mais informações, consulte Excluir máquinas sem acesso ao hipervisor.

Novembro de 2022

Recursos novos e aprimorados

Suporte para entrega de aplicativos MSIX e MSIX app attach. Em **Configuração Completa > Pacotes de Aplicativos**, agora você pode carregar aplicativos empacotados MSIX e MSIX app attach para o Citrix Cloud e entregá-los aos seus usuários. Para obter mais informações, consulte Pacotes de aplicativos.

Aviso para versões de VDA e níveis funcionais não suportados. A interface de Configuração Completa agora alerta você sobre versões de VDA e níveis funcionais não suportados. Para evitar possíveis problemas:

- Se uma máquina executa uma versão de VDA não suportada, você será solicitado a atualizar para uma versão suportada.
- Se o nível funcional de um catálogo ou grupo de entrega não for suportado, você será solicitado a defini-lo para um nível superior.

> **Dica:**

> Os VDAs são cobertos pelos ciclos de vida CR e LTSR do Citrix Virtual Apps and Desktops.

> **Capacidade de anotar imagens mestre estendida à criação de catálogo.** Ao criar um catálogo MCS em **Configuração Completa**, agora você pode anotar sua imagem mestre. Para obter mais informações, consulte Imagem mestre.

Suporte para exportar dados de atribuição de desktop através da Configuração Completa. Ao visualizar atribuições de desktop para um grupo de entrega de SO de sessão única, agora você pode exportar os dados de atribuição para um arquivo CSV para fins de auditoria. Para fazer isso, selecione um grupo de entrega em **Configuração Completa > Grupos de Entrega**, vá para a guia **Desktops** e clique em **Exportar** no canto superior esquerdo da guia.

Guias Todos os Aplicativos e Pastas de Aplicativos consolidadas em uma. Em **Configuração Completa > Aplicativos**, as guias **Todos os Aplicativos** e **Pastas de Aplicativos** foram consolidadas em uma única guia, **Aplicativos**. Essa alteração unifica a experiência do usuário de gerenciamento de visualização de pastas em todos os nós da Configuração Completa.

Suporte para alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada em ambientes Azure. Em ambientes Azure, agora você pode economizar custos de armazenamento alternando o tipo de armazenamento de um disco gerenciado para um nível inferior ao desligar uma VM. Para fazer isso, use a propriedade personalizada `StorageTypeAtShutdown`. O tipo de armazenamento do disco muda para um nível inferior (conforme especificado na propriedade personalizada `StorageTypeAtShutdown`) quando você desliga a VM. Depois de ligar a VM, o tipo de armazenamento volta ao tipo de armazenamento original (conforme especificado na propriedade personalizada `StorageType` ou `WBCDiskStorageType`). Para obter mais informações, consulte Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada.

Atualizações na Visualização de Filtros. A página Filtros no Monitor foi atualizada para incluir listas separadas de filtros Salvos e Padrão para melhor visualização e acessibilidade aos filtros. Você pode selecionar uma visualização entre Máquinas, sessões, Conexões ou Instâncias de Aplicativo. Em seguida, você pode selecionar um filtro da lista de filtros Salvos ou Padrão para visualizar a lista filtrada de dados. Você pode usar as listas suspensas para refinar os critérios de filtro ou editar os critérios existentes. Você pode salvar seu filtro na lista de Filtros Salvos. Para obter mais informações, consulte o artigo Filtros.

Capacidade de redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado por MCS. Em ambientes de virtualização VMware, agora você pode usar o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado por MCS. O recurso automatiza o processo de redefinição do disco do SO. Por exemplo, ele ajuda a redefinir a VM para seu status inicial de um catálogo de desktop de desenvolvimento persistente criado usando MCS.

Para obter mais informações sobre como usar o comando PowerShell para redefinir o disco do SO, consulte Redefinir disco do SO.

Suporte para atualização de perfil de máquina e propriedades personalizadas adicionais de máquinas provisionadas por MCS em ambientes Azure. Anteriormente, em ambientes Azure, você podia usar `Request-ProvVMUpdate` para atualizar a propriedade personalizada `ServiceOffering` de uma máquina provisionada por MCS. Agora, você também pode atualizar o perfil da máquina e as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

Para obter mais informações, consulte Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento.

Suporte para perfil de máquina no GCP. Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS) em ambientes do Google Cloud Platform (GCP), agora você pode usar um perfil de máquina para capturar as propriedades de hardware de uma máquina virtual e aplicá-las às VMs recém-provisionadas no catálogo. Quando o parâmetro `MachineProfile` não é usado, as propriedades de hardware são capturadas da VM da imagem mestre ou do snapshot.

Os perfis de máquina funcionam com os sistemas operacionais Linux e Windows.

Para obter informações sobre como criar um catálogo de máquinas com um perfil de máquina, consulte Criar um catálogo de máquinas usando um perfil de máquina.

Suporte para atualização de máquinas provisionadas por MCS em ambientes GCP. Em ambientes GCP, `Set-ProvScheme` altera o modelo (esquema de provisionamento) e não afeta as máquinas existentes. Usando o comando PowerShell `Request-ProvVMUpdate`, agora você pode aplicar o esquema de provisionamento atual a uma máquina existente (ou conjunto de máquinas). Atualmente, no GCP, a atualização de propriedade suportada por este recurso é o perfil de máquina. Para obter mais informações, consulte Atualizar máquinas provisionadas usando PowerShell.

Outubro de 2022

Recursos novos e aprimorados

Suporte para usar perfis de máquina e grupos de host ao mesmo tempo. Ao criar um catálogo usando uma imagem mestre do Azure Resource Manager, agora você pode usar um perfil de máquina e um grupo de host ao mesmo tempo. Isso é útil em cenários onde você deseja usar o trusted launch para segurança aprimorada e, ao mesmo tempo, executar as máquinas em hosts dedicados. Para obter mais informações, consulte Ambientes de virtualização do Microsoft Azure Resource Manager.

Suporte para organizar grupos de entrega usando pastas. Agora você pode criar uma árvore de pastas para organizar grupos de entrega para facilitar o acesso. Para obter mais informações, consulte Organizar grupos de entrega usando pastas.

Suporte para agendar uma reinicialização única para máquinas através da Configuração Completa. Uma nova opção, **Uma vez**, agora está disponível ao criar agendamentos de reinicialização para grupos de entrega. Com esta opção, você pode agendar máquinas em um grupo de entrega para reiniciar uma vez, em uma data e hora especificadas. Para obter mais informações, consulte Criar um agendamento de reinicialização.

Agendamento Avançado de Sondas. O agendamento aprimorado de Sondas de Aplicativos e Desktops agora pode ser feito a partir do Monitor. Usando este recurso, o Citrix Probe Agent pode ser configurado para executar as tarefas de sonda em dias específicos da semana e repetidas em intervalos especificados durante o dia. Isso permite que você agende uma única tarefa de sonda para se repetir em horários específicos do dia e da semana. Agora você pode verificar proativamente a integridade do seu site com sondas configuradas para serem executadas regularmente em horários adequados. Este recurso simplifica a configuração e o gerenciamento de sondas no Monitor. Para obter mais informações, consulte Sondagem de Aplicativos e Desktops.

Setembro de 2022

Recursos novos e aprimorados

Versões mais antigas do SDK do PowerShell Remoto agora estão obsoletas. Se você estiver usando uma versão obsoleta, o SDK para de funcionar e você verá uma mensagem de erro solicitando que você baixe a versão atual. Se isso acontecer, baixe o SDK do PowerShell Remoto mais recente no site da Citrix.

Catálogos de máquinas com inicialização confiável no Azure. Em ambientes Azure, você pode criar catálogos de máquinas habilitados com inicialização confiável e usar a propriedade `SupportsTrustedLaunch` do inventário de VMs para determinar os tamanhos de VM que suportam a inicialização confiável.

A inicialização confiável é uma maneira contínua de melhorar a segurança das VMs de Geração 2. A inicialização confiável protege contra técnicas de ataque avançadas e persistentes. Para obter mais informações, consulte Catálogos de máquinas com inicialização confiável.

Suporte para identificar recursos do Microsoft System Center Virtual Machine Manager criados pelo MCS. Agora você pode identificar recursos do Microsoft System Center Virtual Machine Manager (SCVMM) criados pelo MCS usando tags. Para obter mais informações sobre as tags que o MCS adiciona aos recursos, consulte Identificar recursos criados pelo MCS.

Suporte para identificar recursos VMware criados pelo MCS. Agora você pode identificar recursos VMware criados pelo MCS usando tags. Para obter mais informações sobre as tags que o MCS adiciona aos recursos, consulte Identificar recursos criados pelo MCS.

Suporte para otimização da limitação do AWS Workspace. Agora você pode ligar e desligar um grande número de máquinas em um AWS Workspace sem encontrar problemas de limitação. Problemas de limitação ocorrem quando o número de solicitações enviadas ao AWS Workspace excede o número de solicitações que o servidor pode manipular. Portanto, a Citrix agora agrupa várias solicitações em uma única solicitação antes de enviá-la ao SDK do AWS Workspace.

Capacidade de verificar detalhes da máquina ao visualizar contagens de máquinas em Início. Ao visualizar contagens de máquinas por estado de disponibilidade em **Início**, agora você pode clicar em um estado para visualizar os detalhes das máquinas nesse estado. Para obter mais informações, consulte Página inicial da interface de Configuração Completa.

Suporte para criação de catálogo de máquinas usando uma imagem de uma assinatura diferente no mesmo locatário do Azure. Anteriormente, em ambientes Azure, você só podia selecionar uma imagem dentro de sua assinatura para criar um catálogo de máquinas. Com este recurso, agora você pode selecionar uma imagem na Azure Compute Gallery (anteriormente Shared Image Gallery) que pertence a uma assinatura compartilhada diferente para criar e atualizar catálogos MCS.

Para obter mais informações sobre a criação de um catálogo, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Para obter informações sobre o compartilhamento de imagem com outro principal de serviço no mesmo locatário, consulte Compartilhamento de imagem com outro principal de serviço no mesmo locatário.

Para obter informações sobre comandos PowerShell para selecionar uma imagem de uma assinatura diferente, consulte Usando PowerShell para selecionar uma imagem de uma assinatura diferente.

Para obter mais informações sobre a Galeria de Computação do Azure, consulte Galeria de Imagens Compartilhadas do Azure.

Agosto de 2022

Recursos novos e aprimorados

Suporte para identificar recursos de hipervisor Citrix criados pelo MCS. Agora você pode identificar recursos de hipervisor Citrix criados pelo MCS usando tags. Para obter mais informações sobre as tags que o MCS adiciona aos recursos, consulte Identificar recursos criados pelo MCS.

Suporte para usar grupos de host e zonas de disponibilidade do Azure ao mesmo tempo. Em ambientes Azure, agora há uma verificação prévia para avaliar se a criação de um catálogo de máquinas será bem-sucedida com base na zona de disponibilidade do Azure especificada na propriedade personalizada e na zona do grupo de host. A criação do catálogo falha se a propriedade personalizada da zona de disponibilidade não corresponder à zona do grupo de host.

Um grupo de host é um recurso que representa uma coleção de hosts dedicados. Um host dedicado é um serviço que fornece servidores físicos que hospedam uma ou mais máquinas virtuais. As zonas de disponibilidade do Azure são locais fisicamente separados dentro de cada região do Azure que são tolerantes a falhas locais.

Para obter mais informações sobre as várias combinações de zona de disponibilidade e zona de grupo de host que resultam na criação bem-sucedida ou falha do catálogo de máquinas, consulte Usando grupos de host e zonas de disponibilidade do Azure ao mesmo tempo.

Suporte para atualização do ID da pasta de um catálogo de máquinas no VMware. Em ambientes de virtualização VMware, agora você pode atualizar o ID da pasta de um catálogo de máquinas MCS usando a propriedade personalizada `FolderID` em `Set-ProvScheme`. As VMs criadas após a atualização do ID da pasta são criadas sob este novo ID de pasta. Se esta propriedade não for especificada em `CustomProperties`, as VMs serão criadas sob a pasta

onde a imagem mestre está localizada. Para obter mais informações sobre a atualização do ID da pasta, consulte Atualizar o ID da pasta de um catálogo de máquinas.

Configuração de fuso horário. Agora você pode configurar o formato de data e hora da interface para atender às suas preferências usando a configuração **Data e hora**. Para obter mais informações, consulte Configuração de fuso horário.

O Image Portability Service (IPS) agora oferece suporte ao Amazon Web Services (AWS). Ao configurar as permissões e componentes necessários para o AWS, os fluxos de trabalho do IPS podem ser usados com uma conta AWS. Consulte Migrar cargas de trabalho para a nuvem pública para obter mais detalhes.

Configuração do arquivo de paginação durante a preparação da imagem em ambientes Azure. Em ambientes Azure, agora você pode evitar confusão potencial com o local do arquivo de paginação. Para isso, o MCS agora determina sua localização ao criar o esquema de provisionamento durante a preparação da imagem. Este cálculo é baseado em certas regras. Recursos como disco de SO efêmero (EOS) e MCS I/O têm seu próprio local de arquivo de paginação esperado e são exclusivos entre si. Além disso, se você desvincular a preparação da imagem da criação do esquema de provisionamento, o MCS determinará corretamente onde ele deve estar. Para obter mais informações sobre o local do arquivo de paginação, consulte Local do arquivo de paginação.

Suporte para atualização da configuração do arquivo de paginação em ambientes Azure. Ao criar um catálogo em um ambiente Azure, agora você pode especificar a configuração do arquivo de paginação, incluindo seu local e tamanho, usando comandos PowerShell. Isso substitui a configuração do arquivo de paginação determinada pelo MCS. Você pode fazer isso executando o comando `New-ProvScheme` com as seguintes propriedades personalizadas:

- `PageFileDiskDriveLetterOverride`: Letra da unidade de disco do local do arquivo de paginação
- `InitialPageFileSizeInMB`: Tamanho inicial do arquivo de paginação em MB
- `MaxPageFileSizeInMB`: Tamanho máximo do arquivo de paginação em MB

Para obter mais informações sobre como atualizar a configuração do arquivo de paginação, consulte Atualizar configuração do arquivo de paginação.

Atualizações na página inicial. O widget Introdução agora tem uma nova aparência. Outras atualizações na página inicial incluem:

- Os ícones de Atualizar e Ajuda recém-adicionados no canto superior direito.

- Contagens de recursos clicáveis, fornecendo acesso rápido a páginas de recursos relevantes.
- Melhoria no ícone Não gostei. Se você não gostar de uma recomendação, a recomendação desaparecerá. Se você não gostar do widget de recomendação, o widget desaparecerá.

Para obter mais informações, consulte Página inicial.

Suporte para habilitar extensões de VM do Azure. Ao usar uma especificação de modelo ARM como um perfil de máquina para criar um catálogo de máquinas, agora você pode adicionar extensões de VM do Azure às VMs no catálogo, visualizar a lista de extensões suportadas e remover as extensões que você adicionou. As extensões de VM do Azure são pequenos aplicativos que fornecem configuração pós-implantação e tarefas de automação em VMs do Azure. Por exemplo, se uma VM requer instalação de software, proteção antivírus ou a capacidade de executar um script dentro dela, você pode usar uma extensão de VM. Para obter mais informações sobre como habilitar extensões de VM do Azure, consulte Usar o PowerShell para habilitar extensões de VM do Azure.

Suporte a inicialização confiável para disco de SO efêmero. Agora você pode criar esquemas de provisionamento usando disco de SO efêmero no Windows com inicialização confiável. A inicialização confiável é uma maneira contínua de melhorar a segurança das VMs de geração 2. Ela protege contra técnicas de ataque avançadas e persistentes, combinando tecnologias que podem ser habilitadas independentemente, como inicialização segura e versão virtualizada do módulo de plataforma confiável (vTPM). Para obter mais informações sobre como criar um catálogo de máquinas, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Julho de 2022

Recursos novos e aprimorados

Tempos limite de sessão dinâmicos para máquinas de SO de sessão única. Os tempos limite de sessão dinâmicos agora suportam máquinas de SO de sessão única. É necessário um grupo de entrega com pelo menos um VDA da versão 2206 ou posterior. Certifique-se de que esses VDAs tenham se registrado no Citrix Cloud pelo menos uma vez. Para obter mais informações, acesse Tempos limite de sessão dinâmicos.

Enviar lembretes de logoff sem forçar o logoff do usuário no Autoscale. Um novo recurso está agora disponível em **Notificações de Logoff do Usuário** (anteriormente **Forçar Logoff do Usuário**) no Autoscale. O recurso permite enviar lembretes de logoff aos usuários sem forçá-los a

fazer logoff. Isso evita a potencial perda de dados causada por forçar os usuários a fazer logoff de suas sessões. Consulte Notificações de logoff do usuário para obter detalhes.

Capacidade de definir o tipo de licença do SO Linux ao criar catálogos de VM Linux no Azure. Usando a interface de Configuração Completa, agora você pode escolher o tipo de licença do SO Linux ao criar catálogos de VM Linux no Azure. Você tem duas opções para licenças Linux próprias: Red Hat Enterprise Linux e SUSE Linux Enterprise Server. Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Experiência de pesquisa aprimorada na Configuração Completa. O nó Pesquisa oferece os seguintes novos recursos e aprimoramentos:

- **Capacidade de exportar resultados de pesquisa**. Agora você pode exportar resultados de pesquisa. Para fazer isso, clique no ícone de exportação no canto superior direito.
- **Novo filtro disponível**. Um filtro, Ação de Energia Pendente, está agora disponível para uso. Use o filtro para refinar sua pesquisa.
- **Suporte à pesquisa "Não contém" para certos itens**. Itens como nomes de máquinas e tags agora suportam critérios de pesquisa "Não contém".
- **Suporte para pesquisa de objetos ao adicionar filtros**. Ao adicionar filtros para os seguintes objetos, agora você pode pesquisá-los: conexões, catálogos de máquinas, grupos de entrega, grupos de aplicativos e tags.

Para obter mais informações, consulte Usar Pesquisa na interface de gerenciamento de Configuração Completa.

Suporte para perfis de armazenamento VMware. Ao criar um catálogo de máquinas usando uma imagem mestre em um Datastore vSAN, agora você pode copiar a política de armazenamento, como as informações RAID-1 ou RAID-5, da imagem mestre para os dispositivos de destino criados. Para catálogos existentes, a política de armazenamento permanece inalterada mesmo se você atualizar o catálogo.

Suporte para registro de SPN RestrictedKrbHost. Todas as contas de computador criadas pelo Citrix MCS agora são registradas com `RestrictedKrbHost` Nomes de Entidade de Serviço (SPN). Isso evita a necessidade de executar o comando `setspn` para registrar o SPN para as contas de computador depois que o MCS as cria.

Pacotes de aplicativos na Configuração Completa para entrega de aplicativos empacotados da Microsoft. O nó App-V é renomeado para Pacotes de Aplicativos e redesenhado para acomodar mais tipos de aplicativos empacotados da Microsoft. Anteriormente, você precisava usar o módulo de descoberta para adicionar aplicativos empacotados App-V ao seu ambiente para

entrega. Agora você pode adicionar e entregar os aplicativos em um só lugar usando o nó Pacotes de Aplicativos. Para obter mais informações, consulte Pacotes de aplicativos.

Suporte para usar especificações de modelo ARM como perfis de máquina. Anteriormente, você podia usar apenas VMs como perfis de máquina. Agora você também pode usar especificações de modelo ARM como perfis de máquina ao criar catálogos de máquinas Azure. Este recurso permite que você aproveite os recursos de modelo Azure ARM, como o controle de versão. Para garantir que a especificação selecionada esteja configurada corretamente e contenha as configurações necessárias, realizamos uma validação nela. Se a validação falhar, você será solicitado a selecionar um perfil de máquina diferente. Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Suporte para validação de especificação de modelo ARM. Agora você pode validar a especificação de modelo ARM para garantir que ela possa ser usada como um perfil de máquina para criar um catálogo de máquinas. Existem duas maneiras de validar a especificação de modelo ARM:

- Usando a interface de gerenciamento de Configuração Completa.
- Usando o comando PowerShell.

Para obter mais informações sobre a validação da especificação de modelo ARM, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Junho de 2022

Recursos novos e aprimorados

Suporte a agendamento de reinicialização para máquinas de SO de sessão única. Anteriormente, o recurso de agendamento de reinicialização estava disponível apenas para máquinas de SO de várias sessões. Agora, ele também está disponível para máquinas de SO de sessão única. Agora você pode criar agendamentos de reinicialização para grupos de entrega que contêm máquinas de SO de sessão única. Para obter mais informações, consulte Criar e gerenciar agendamentos de reinicialização para máquinas em um grupo de entrega.

Opção para realizar pré-verificações de nome de usuário. Uma opção, **Verificar nome**, agora está disponível ao inserir credenciais de domínio. Com a opção, você pode verificar se o nome de usuário é válido ou exclusivo. A opção é útil, por exemplo, quando:

- O mesmo nome de usuário existe em vários domínios. Você é solicitado a selecionar o usuário desejado.

- Você não consegue se lembrar do nome de domínio. Você pode inserir o nome de usuário sem especificar o nome de domínio. Se a verificação for aprovada, o nome de domínio será preenchido automaticamente.

Para obter mais informações, consulte Credenciais de domínio.

Capacidade de alterar a configuração de rede para um esquema de provisionamento existente. Agora você pode alterar a configuração de rede para um esquema de provisionamento existente para que as novas VMs sejam criadas na nova sub-rede. Use o parâmetro `-NetworkMapping` no comando `Set-ProvScheme` para alterar a configuração de rede. Somente as VMs recém-provisionadas do esquema terão as novas configurações de sub-rede. Você também deve garantir que as sub-redes estejam na mesma unidade de hospedagem. Para obter mais informações, consulte Alterar a configuração de rede para um esquema de provisionamento existente.

Recuperar informações de nome de região para VMs do Azure, discos gerenciados, instantâneos, VHD do Azure e modelo ARM. Agora você pode exibir as informações de nome de região para uma VM do Azure, discos gerenciados, instantâneos, VHD do Azure e modelo ARM. Essas informações são exibidas para os recursos na imagem mestre quando um catálogo de máquinas é atribuído. Para obter mais informações, consulte Recuperar informações de nome de região para VMs do Azure, discos gerenciados, instantâneos, VHD do Azure e modelo ARM.

Capacidade de usar valores de propriedade de perfil de máquina no ambiente do Azure. Ao criar um catálogo do Azure com um perfil de máquina, agora você pode definir os valores de propriedade da especificação do modelo ARM ou da VM, o que for usado como perfil de máquina, se os valores não forem explicitamente definidos nas propriedades personalizadas. As propriedades afetadas por este recurso são:

- Zona de disponibilidade
- ID do Grupo de Host Dedicado
- ID do Conjunto de Criptografia de Disco
- Tipo de SO
- Tipo de licença
- Oferta de Serviço
- Tipo de armazenamento

Se algumas das propriedades estiverem faltando no perfil da máquina e não estiverem definidas nas propriedades personalizadas, o valor padrão das propriedades será aplicado onde for

aplicável. Para obter mais informações, consulte Usar valores de propriedade de perfil de máquina.

Suporte estendido para atualização de VDA. Usando a interface de Configuração Completa, agora você pode atualizar máquinas persistentes provisionadas por MCS. Você pode atualizá-las por catálogo ou por máquina. Para obter mais informações, consulte Atualizar VDAs usando a interface de Configuração Completa.

Citrix Probe Agent em Citrix Cloud Japan e Citrix Cloud Government Control Planes. O Citrix Probe Agent agora oferece suporte a sites hospedados em Citrix Cloud Japan e Citrix Cloud Government Control Planes. Para usar o agente de sondagem nesses planos, defina o valor do registro no caminho "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" como 2 para o Japão e 3 para a região do Governo. O Citrix Probe Agent automatiza o processo de verificação da integridade de aplicativos e desktops virtuais publicados em um site. Para obter mais informações, consulte Sondagem de Aplicativos e Desktops.

Personalize a porta usada para comunicação entre VDAs e Cloud Connectors. Agora você pode personalizar a porta que o VDA usa para se comunicar com os Cloud Connectors com base em seus requisitos de segurança específicos. Esse recurso é útil se sua equipe de segurança não permite que a porta padrão (porta 80) esteja aberta ou se a porta padrão já estiver em uso. Para obter mais informações, consulte Personalizar a porta para comunicação com Cloud Connectors.

Suporte para organização de catálogos de máquinas usando pastas. Agora você pode criar pastas aninhadas para organizar catálogos de máquinas para facilitar o acesso. Para obter mais informações, consulte Organizar catálogos usando pastas.

Suporte para SCVMM 2022. O Citrix DaaS agora oferece suporte ao System Center Virtual Machine Manager (SCVMM) 2022 da Microsoft. O SCVMM fornece uma variedade de serviços para incluir a manutenção dos recursos necessários para implantar VMs. Para obter mais informações sobre os novos recursos suportados no SCVMM 2022, consulte Novidades no System Center Virtual Machine Manager.

Suporte para configuração do parâmetro de operações de provisionamento simultâneas máximas no AWS. O Citrix DaaS agora oferece suporte a `MaximumConcurrentProvisioningOperations` como uma propriedade personalizada configurável para MCS no AWS. `MaximumConcurrentProvisioningOperations` é a propriedade que determina o número de VMs que você pode criar ou excluir simultaneamente. Embora o MCS suporte 100 operações de provisionamento simultâneas máximas por padrão, agora você pode inserir comandos PowerShell para personalizar esse valor. Você pode inserir um

intervalo de 1 a 1000. Definir essa propriedade para o seu valor preferido permite controlar o número de tarefas paralelas que você pode executar ao criar ou excluir VMs. Para obter detalhes sobre como configurar as operações de provisionamento simultâneas máximas, consulte Valores Padrão de Conexão do Host.

Maio de 2022

Recursos novos e aprimorados

Diagnóstico aprimorado de inicialização de sessão. O Citrix DaaS agora oferece suporte a diagnósticos detalhados de falha na inicialização de sessão. Agora você pode visualizar os componentes envolvidos na sequência de inicialização da sessão. Os componentes que falharam com os últimos códigos de erro gerados são destacados. Isso ajuda a identificar a razão exata para uma falha na inicialização da sessão e tomar a ação recomendada.

A página Transação é estendida com o painel Detalhes da Transação que contém uma lista de componentes indicando a ocorrência do erro. Clicar no nome do componente exibe os Detalhes do Componente e os Detalhes da Última Falha Conhecida. A Razão da Falha e o Código de Erro são exibidos. Clicar no link Saiba mais leva ao código específico em Códigos de erro contendo uma descrição detalhada e a ação recomendada. Para obter mais informações, consulte Diagnóstico de Sessão.

Suporte para usar Set-ProvServiceConfigurationData no Remote PowerShell SDK. Agora você pode executar `Set-ProvServiceConfigurationData` usando o Remote PowerShell SDK para fazer as configurações em todos os parâmetros aplicáveis. Você também pode pular a habilitação do DHCP durante a preparação da imagem usando este comando. A seguir está a lista de configurações suportadas com `Set-ProvServiceConfigurationData`:

- Alterar Tempo Limite de Preparação da Imagem: `Set-ProvServiceConfigurationData -Name "ImageManagementPrep_PreparationTimeout" -value 60`
- Ignorar Habilitação de DHCP: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value EnableDHCP`
- Ignorar Rearm do Microsoft Windows KMS: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm`
- Ignorar Rearm do KMS do Microsoft Office: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OfficeRearm`

- Desativar desligamento automático da VM de preparação: `Set-ProvServiceConfigurationData –Name ImageManagementPrep_NoAutoShutdown –Value true`
- Desativar injeção de domínio: `Set-ProvServiceConfigurationData –Name DisableDomainInjection –Value true`

Capacidade de definir o tipo de licença Linux ao criar catálogos de máquinas Linux usando comandos PowerShell. Usando comandos PowerShell, você pode definir o tipo de licença Linux ao criar catálogos de máquinas Linux. Você tem duas opções para licenças Linux próprias: RHEL_BYOS e SLES_BYOS. A configuração padrão é o licenciamento Azure Linux. Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Suporte para identificar todos os recursos do Azure criados pelo MCS. Agora você pode identificar todos os recursos do Azure criados pelo MCS, como Imagem, disco de ID, disco do SO, NIC, VM e assim por diante, que estão associados a um ProvScheme usando uma tag chamada `provschemeID`. Para obter mais informações sobre as tags que o MCS adiciona aos recursos, consulte Identificar recursos criados pelo MCS.

Suporte para adicionar usuários não-Active Directory manualmente. Usando a interface de gerenciamento de Configuração Completa, agora você pode inserir uma lista de nomes de usuário separados por ponto e vírgula ao adicionar usuários não-Active Directory para um catálogo. Considere o formato ao adicionar usuários que residem em diretórios diferentes. Por exemplo, se os usuários estiverem no Active Directory, insira os nomes diretamente. Caso contrário, insira os nomes neste formato: `<identity provider>:<user name>`. Exemplo: `AzureAD:username`. Para obter mais informações, consulte Criar catálogo de máquinas.

Abril de 2022

Novos recursos e aprimoramentos

Página inicial para a interface de Configuração Completa. A Configuração Completa agora tem uma página inicial, que fornece uma visão geral da sua implantação e cargas de trabalho do Citrix DaaS, juntamente com informações que o ajudam a aproveitar ao máximo sua assinatura. A página é composta pelas seguintes partes:

- **Visão geral do serviço**. Fornece uma visão geral da sua implantação e cargas de trabalho do Citrix DaaS.

- **Recomendações**. Recomenda recursos disponíveis com sua assinatura e coleta seu feedback.
- **Novidades**. Mostra os recursos mais recentes.
- **Recursos de visualização**. Mostra os recursos que estão atualmente em visualização.
- **Introdução**. Mostra as etapas para guiá-lo pela configuração inicial.

Para obter mais informações, consulte Página inicial.

Mostrar o progresso da criação e atualização de catálogos. A Configuração Completa agora permite que você se mantenha atualizado sobre a criação e as atualizações de catálogos. Você pode obter uma visão geral do processo de criação e atualização, visualizar o histórico das etapas realizadas e monitorar o progresso e o tempo de execução da etapa atual. Para obter mais informações, consulte Iniciar a criação do catálogo.

Exibir hipervisores e serviços de nuvem disponíveis com base na zona selecionada. Na Configuração Completa, ao criar conexões de hospedagem, é necessário selecionar uma zona antes de selecionar um tipo de conexão. A lista suspensa Tipo de conexão exibe os hipervisores e serviços de nuvem disponíveis com a zona. Anteriormente, para garantir que a lista Tipo de conexão mostrasse um hipervisor ou serviço de nuvem necessário, você precisava instalar seu plug-in em todas as zonas. Com esta nova sequência de configuração, agora você pode instalar o plug-in apenas na zona necessária.

Você também pode usar o comando PowerShell para obter a lista de plug-ins de hipervisor disponíveis com a zona selecionada. Para obter mais informações, consulte Criar uma conexão e recursos.

Suporte para usuários não associados ao AD local na Configuração Completa. Um novo campo, **Selecionar tipo de identidade**, está disponível nas interfaces onde você atribui usuários a desktops ou aplicativos provisionados, grupos de entrega ou grupos de aplicativos. Com o campo, agora você pode selecionar contas de usuário de qualquer um dos seguintes provedores de identidade aos quais seu Citrix Cloud está conectado:

- Active Directory
- Azure Active Directory
- Okta

Capacidade de rejeitar propriedades personalizadas inválidas em ambientes Google Cloud Platform (GCP) e Azure. Agora você pode evitar confusão potencial se as propriedades personalizadas definidas em `New-ProvScheme` e `Set-ProvScheme` não entrarem em vigor. Se

você especificar uma propriedade ou propriedades personalizadas não existentes, receberá uma mensagem de erro. Para obter mais informações, consulte Consideração importante sobre a configuração de propriedades personalizadas.

Suporte para a criação de máquinas associadas ao Azure Active Directory. Na **Configuração Completa**, ao criar um catálogo, um tipo de identidade **Associado ao Azure Active Directory** agora está disponível em **Identidades de Máquina**. Com esse tipo de identidade, você pode usar o MCS para criar máquinas que são associadas ao Azure Active Directory. Você também tem uma opção extra, **Registrar as máquinas no Microsoft Intune**, para registrar as máquinas no Microsoft Intune para gerenciamento.

Para obter informações sobre a criação de catálogos associados ao Azure Active Directory, consulte Criar catálogos de máquinas. Para obter informações sobre requisitos e considerações relacionadas à associação ao Azure Active Directory, consulte Associado ao Azure Active Directory.

Suporte para a criação de máquinas associadas ao Azure Active Directory híbrido. Na **Configuração Completa**, ao criar um catálogo, um tipo de identidade **Associado ao Azure Active Directory híbrido** agora está disponível em **Identidades de Máquina**. Com esse tipo de identidade, você pode usar o MCS para criar máquinas associadas ao Azure Active Directory híbrido. Essas máquinas são de propriedade de uma organização e são acessadas com uma conta do Active Directory Domain Services que pertence a essa organização.

Para obter informações sobre a criação de catálogos associados ao Azure Active Directory híbrido, consulte Criar catálogos de máquinas. Para obter informações sobre requisitos e considerações relacionadas à associação ao Azure Active Directory híbrido, consulte Associado ao Azure Active Directory híbrido.

Suporte ao lançamento confiável do Azure para snapshots. Além das imagens, o lançamento confiável do Azure agora também está disponível para snapshots. Se você selecionar um snapshot com o lançamento confiável ativado, o uso de um perfil de máquina é obrigatório. Além disso, você deve selecionar um perfil de máquina com o lançamento confiável ativado. Para obter mais informações, consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

Exportar máquinas. Agora você pode exportar as máquinas listadas na página **Máquinas** do assistente **Configuração do Catálogo de Máquinas** para um arquivo CSV, para ser usado como um modelo ao adicionar máquinas a um catálogo em massa. Para obter mais informações, consulte Exportar máquinas de um catálogo.

Opção para acessar o console web do Workspace Environment Management. Uma opção, Gerenciamento de Ambiente (Web), agora está disponível no menu da guia **Gerenciar**. A opção leva você ao novo console web do Workspace Environment Management. Para acessar o console legado, use **Gerenciamento de Ambiente**. Estamos em processo de migração de todo o conjunto de funcionalidades do console legado para o console web. O console web geralmente responde mais rápido que o console legado. Para obter mais informações, consulte Serviço Workspace Environment Management.

Capacidade de gerenciar parâmetros ProvScheme. Ao usar o MCS para criar um catálogo, agora você receberá um erro se definir os parâmetros `New-ProvScheme` em hipervisores não suportados durante a criação do catálogo de máquinas ou atualizar os parâmetros `Set-ProvScheme` após a criação do catálogo de máquinas. Para obter mais informações, consulte Criar catálogos de máquinas.

Limites de localização de recursos aumentados. Os limites de localização de recursos para VDAs de sessão única e VDAs de múltiplas sessões foram aumentados para 10000 e 1000, respectivamente. Para obter mais informações, consulte Limites.

Suporte para reiniciar máquinas não gerenciadas por energia após o esgotamento de todas as sessões. O Citrix DaaS agora permite criar agendamentos de reinício para máquinas que não são gerenciadas por energia após todas as sessões serem esgotadas das máquinas. Na interface de Configuração Completa, selecione **Reiniciar todas as máquinas após o esgotamento de todas as sessões** como a **Duração do reinício**. Para obter mais informações, consulte Criar um agendamento de reinício.

Suporte para atualização de máquinas VDA (visualização). Usando a interface de Configuração Completa, agora você pode atualizar máquinas VDA para sua implantação do Citrix DaaS. Você pode atualizá-las por catálogo ou por máquina. O recurso se aplica a máquinas que não são criadas usando MCS (por exemplo, máquinas físicas). Para obter mais informações, consulte Atualizar VDAs usando a interface de Configuração Completa.

Máquinas não são desligadas durante interrupções. O Citrix DaaS agora impede que as máquinas virtuais sejam desligadas pelo broker quando a zona em que as máquinas estão sofre uma interrupção. As máquinas ficam automaticamente disponíveis para conexões quando a interrupção termina. Você não precisa tomar nenhuma ação para tornar as máquinas disponíveis após a interrupção.

Diagnóstico de inicialização de sessão. O Citrix DaaS agora oferece suporte a diagnósticos aprimorados de falha na inicialização de sessão. Use o ID de Transação de 32 dígitos (8-4-4-4-12) gerado pelo aplicativo Citrix Workspace de dentro do Citrix Monitor (ou seja, serviço Citrix Director)

para identificar o componente e o estágio exatos onde o problema ocorreu e aplicar as ações recomendadas para resolver o problema. Para obter mais informações, consulte Diagnóstico de inicialização de sessão.

Opção para acessar o serviço de Gravação de Sessão. Uma opção, Gravação de Sessão, agora está disponível no menu da guia **Gerenciar**. A introdução do serviço de Gravação de Sessão oferece gerenciamento centralizado de políticas, reprodução e configurações de servidor. Isso alivia a carga sobre os administradores de TI, fornecendo um ponto de entrada unificado para gerenciar e observar os objetos distribuídos em sua organização. Para obter mais informações, consulte Serviço de Gravação de Sessão (visualização).

Serviço Citrix Virtual Apps and Desktops renomeado. Citrix Virtual Apps and Desktops service foi renomeado para **Citrix DaaS**. Saiba mais sobre a mudança de nome em nosso anúncio em nosso blog.

As seguintes ofertas do serviço Citrix Virtual Apps and Desktops foram renomeadas.

- **Citrix Virtual Apps service Advanced** renomeado para **Citrix DaaS Advanced**.
- **Citrix Virtual Apps service Premium** renomeado para **Citrix DaaS Premium**.
- **Citrix Virtual Desktops™ service** renomeado para **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops service Advanced** renomeado para **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops service Premium** agora disponível como **Citrix DaaS Premium e Citrix DaaS Premium Plus**.
- **Citrix Virtual Apps and Desktops Standard for Azure** renomeado para **Citrix DaaS Standard for Azure**.
- **Citrix Virtual Apps and Desktops Standard for Google Cloud** renomeado para **Citrix DaaS Standard for Google Cloud**.
- **Citrix Virtual Apps and Desktops Premium for Google Cloud** renomeado para **Citrix DaaS Premium for Google Cloud**.

A implementação dessa transição em nossos produtos e sua documentação é um processo contínuo. Agradecemos sua paciência durante essa transição.

- A interface do usuário do produto, o conteúdo do produto e as imagens e instruções na documentação do produto serão atualizados nas próximas semanas.
- É possível que alguns itens (como comandos e MSIs) continuem a manter seus nomes anteriores para evitar quebrar scripts de clientes existentes.

- A documentação do produto relacionada e outros recursos (como vídeos e postagens de blog) que estão vinculados a esta documentação do produto ainda podem conter nomes antigos.

Nota:

O nome do produto **Citrix Virtual Apps and Desktops** local permanece o mesmo.

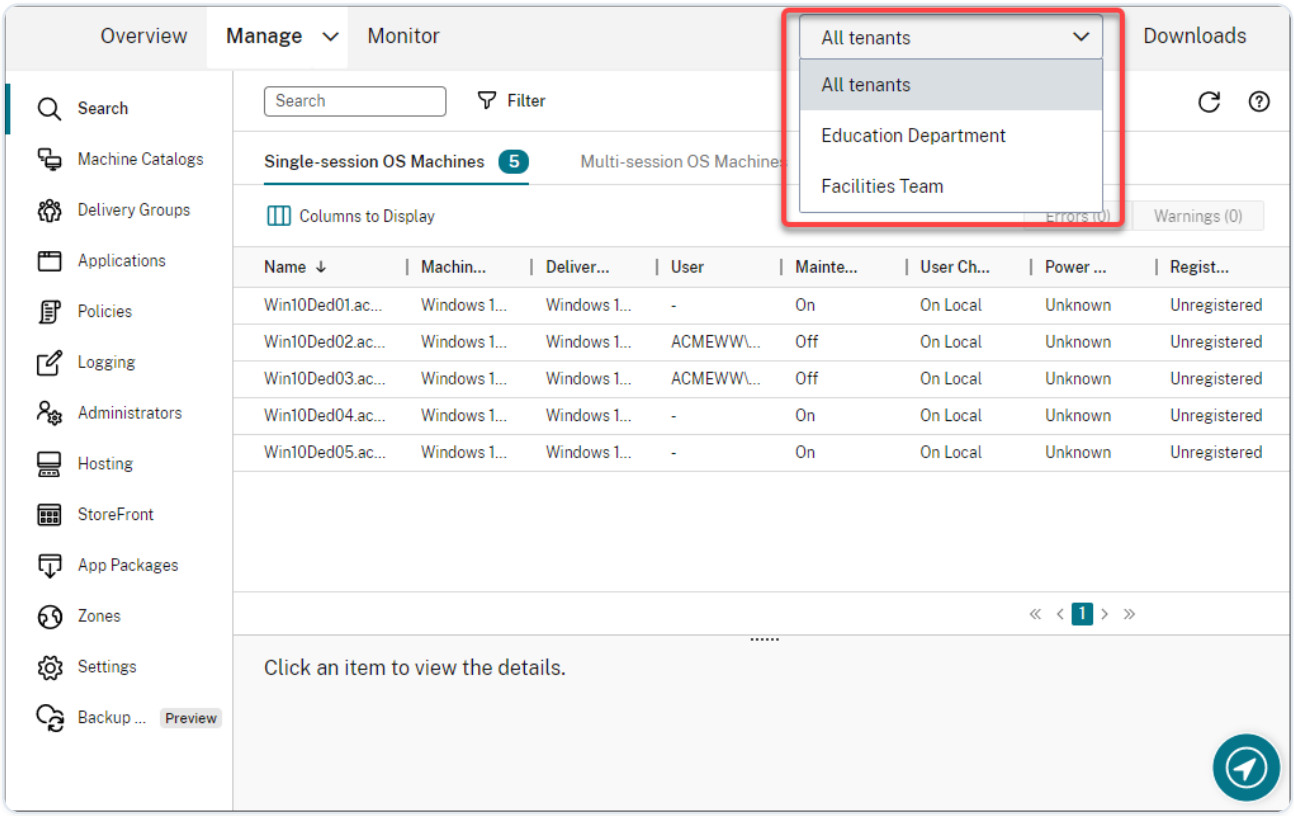
Suporte a locatários na Configuração Completa. Agora você pode criar partições de configuração em uma única instância do Citrix DaaS. Você consegue isso criando escopos de locatário em **Administradores > Escopos** e associando objetos de configuração relacionados, como catálogos de máquinas e grupos de entrega, a esses locatários. Como resultado, os administradores com acesso a um locatário podem gerenciar apenas objetos associados a esse locatário. Esse recurso é útil, por exemplo, se sua organização:

- Possui diferentes silos de negócios (divisões independentes ou equipes de gerenciamento de TI separadas) ou
- Possui vários sites locais e deseja manter a mesma configuração em uma única instância do Citrix DaaS.

Além disso, a interface de Configuração Completa permite filtrar clientes locatários por nome. Por padrão, a interface exibe informações sobre todos os locatários.

O recurso está disponível para Provedores de Serviços Citrix (CSPs) e não-CSPs. A interface em um ambiente CSP é essencialmente a mesma que em um ambiente não-CSP, exceto pelo método usado para criar locatários.

- Os CSPs integram clientes locatários ao Citrix DaaS e, em seguida, configuram o acesso de administrador ao Citrix DaaS. Para obter mais informações, consulte Citrix DaaS para Provedores de Serviços Citrix.
- Não-CSPs criam clientes locatários primeiro criando escopos e, em seguida, configurando acesso personalizado para os respectivos administradores. Para obter mais informações, consulte Criar e gerenciar escopos.



Atualizações para o Autoscale. Atualizamos o Autoscale com um estilo de lâmina para oferecer uma melhor experiência do usuário. Os fluxos de trabalho para configurar suas definições permanecem os mesmos. Outras atualizações para o Autoscale incluem:

- Renomeado **Restringir Autoscale** para **Dimensionamento Automático de Máquinas Marcadas** para facilitar o entendimento.
- Adicionada uma nova opção, **Controlar quando o Autoscale começa a ligar máquinas marcadas**. A opção permite controlar quando o Autoscale começa a ligar máquinas marcadas com base no uso de máquinas não marcadas.

Para obter mais informações sobre o dimensionamento automático de máquinas marcadas, consulte Dimensionamento automático de máquinas marcadas.

Verificações de validade da licença. A interface de Configuração Completa agora verifica automaticamente a validade das licenças em uso pelas conexões de host. Uma conexão de host é colocada em modo de manutenção se sua licença for inválida. Como resultado, você não pode realizar certas operações, como editar a conexão e desativar o modo de manutenção. Uma licença se torna inválida, por exemplo, quando:

- A licença expirou. Nesse caso, entre em contato com seu representante de vendas da Citrix para renová-la ou para adquirir novas licenças.
- A licença foi excluída do Servidor de Licenças.

Estilo de lâmina aplicado aos nós de Catálogos de Máquinas e Políticas. Os estilos de lâmina agora são aplicados a todos os nós da Configuração Completa.

Suporte para atualização de máquinas provisionadas por MCS em ambientes Azure. `Set-ProvScheme` altera o modelo (esquema de provisionamento) e não afeta as máquinas existentes. Usando o comando Request-ProvVMUpdate, agora você pode aplicar o esquema de provisionamento atual a uma máquina existente (ou conjunto de máquinas). Atualmente, a atualização de propriedade suportada por este recurso é `ServiceOffering`. Para obter mais informações, consulte Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento.

Março de 2022

Recursos novos e aprimorados

Citrix Virtual Apps and Desktops para Google Cloud disponível no Google Cloud Marketplace. O Citrix Virtual Apps and Desktops Premium para Google Cloud agora está disponível para compra no Google Cloud Marketplace. O Citrix Virtual Apps and Desktops Premium para Google Cloud executa o plano de controle do serviço Citrix Virtual Apps and Desktops no Google Cloud.

Suporte para inicialização confiável do Azure. A inicialização confiável do Azure agora está disponível para a interface de gerenciamento de Configuração Completa. Se você optar por selecionar uma imagem com inicialização confiável ativada, o uso de um perfil de máquina é obrigatório. Além disso, você deve selecionar um perfil de máquina com inicialização confiável ativada. Para obter mais informações, consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

Estilo de lâmina aplicado a assistentes em mais três nós na Configuração Completa. Os nós são **Pesquisa**, **Grupos de Entrega** e **Aplicativos**.

O Image Portability Service (IPS) foi lançado para disponibilidade geral. O IPS simplifica o gerenciamento de imagens entre plataformas. Este recurso é útil para gerenciar imagens entre um local de recurso local e a nuvem pública. As APIs REST do Citrix Virtual Apps and Desktops podem ser usadas para automatizar a administração de recursos em um site do Citrix Virtual Apps and Desktops. Para obter mais informações, consulte Migrar cargas de trabalho para a nuvem pública.

Fevereiro de 2022

Recursos novos e aprimorados

Permissões do Azure. Existem dois conjuntos de permissões necessárias para requisitos de segurança e para minimizar riscos.

- Permissões mínimas: Este conjunto de permissões oferece melhor controle de segurança. No entanto, novos recursos que exigem permissões adicionais falharão devido ao uso de permissões mínimas.
- Permissões gerais: Este conjunto de permissões não impede que você obtenha o benefício de novos aprimoramentos.

Para obter mais informações, consulte Sobre as permissões do Azure.

Suporte para usar o disco temporário da VM para hospedar o disco de cache de write-back em ambientes Azure. Adicionamos uma opção, **Usar disco de cache de write-back não persistente**, à página **Configuração do Catálogo de Máquinas > Configurações de Disco** da interface **Gerenciar > Configuração Completa**. Selecione essa opção se você não quiser que o disco de cache de write-back persista para as VMs provisionadas. Com a opção selecionada, usamos o disco temporário da VM para hospedar o disco de cache de write-back se o disco temporário tiver espaço suficiente. Isso reduz seus custos. Para obter mais informações, consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

Atualizações nas configurações padrão de conexão de host do AWS. Os valores das configurações padrão de conexão de host do AWS são atualizados para valores mais altos e provavelmente são os mesmos para todas as configurações da plataforma de nuvem AWS. Isso ajuda a criar conexões de host em ambientes de nuvem AWS, sem avaliar e configurar os valores das configurações padrão de acordo com a configuração individual. Para obter mais informações, consulte Valores padrão de conexão de host.

Adicionado suporte para diferentes camadas de armazenamento em ambientes GCP. Agora você pode fornecer as seguintes propriedades personalizadas nos ambientes GCP para definir o tipo de armazenamento dos discos anexados à VM recém-criada:

- StorageType
- IdentityDiskStorageType
- WBCDiskStorageType

Para obter mais informações, consulte SDK do Serviço Citrix Virtual Apps and Desktops.

Alterar certas configurações de VM após a criação de catálogos de VM do Azure. Usando a interface de gerenciamento de Configuração Completa, agora você pode alterar as seguintes configurações após a criação de um catálogo:

- Tamanho da máquina
- Zonas de disponibilidade
- Perfil da máquina
- Licenças do Windows

Para fazer isso, no nó **Catálogos de Máquinas**, selecione o catálogo e, em seguida, selecione **Editar Catálogo de Máquinas** na barra de ações. Para obter mais informações, consulte Editar um catálogo.

Suporte para armazenar o disco do SO efêmero do Azure no disco de cache ou no disco temporário. O serviço Citrix Virtual Apps and Desktops agora permite que você armazene o disco do SO efêmero do Azure no disco de cache ou no disco temporário para uma máquina virtual habilitada para Azure. Essa funcionalidade é útil para ambientes Azure que exigem um disco SSD de maior desempenho em vez de um disco HDD padrão. Para obter mais informações, consulte Ambientes de nuvem do Microsoft Azure Resource Manager.

Suporte para clusters Nutanix no AWS. O serviço Citrix Virtual Apps and Desktops oferece suporte a clusters Nutanix no AWS. Os clusters Nutanix simplificam a forma como os aplicativos são executados em nuvens privadas ou em várias nuvens públicas. Para obter mais informações, consulte Clusters Nutanix no AWS.

Suporte para VMware Cloud no Amazon Web Services (AWS). O VMware Cloud no Amazon Web Services (AWS) permite migrar cargas de trabalho Citrix locais baseadas em VMware para a nuvem AWS e seu ambiente principal do Citrix Virtual Apps and Desktops para o serviço Citrix Virtual Apps and Desktops. Para obter mais informações, consulte VMware Cloud no Amazon Web Services (AWS).

Suporte para configurar o disco de cache de write-back para máquinas em execução no Google Cloud Platform (GCP). Na interface de gerenciamento de Configuração Completa, ao provisionar máquinas no GCP, agora você pode configurar as seguintes configurações de disco de cache de write-back:

- Tamanho do disco
- Memória alocada para o cache
- Tipo de armazenamento em disco

- Persistência do disco

Para obter mais informações, consulte Criar um catálogo de máquinas no artigo Ambientes de virtualização do Google Cloud Platform.

Janeiro de 2022

Recursos novos e aprimorados

Suporte para clusters Nutanix no AWS. O serviço Citrix Virtual Apps and Desktops agora oferece suporte a clusters Nutanix no AWS. Este suporte oferece a mesma funcionalidade de um cluster Nutanix local. Apenas um único cluster é suportado, *Prism Element*. Para obter mais informações, consulte Ambientes de virtualização Nutanix.

Novos recursos disponíveis no Cloud Health Check. O Cloud Health Check foi atualizado para uma nova versão com recursos que incluem:

- **Correção automática.** O Cloud Health Check agora oferece suporte à detecção e correção automática de certos problemas identificados em máquinas onde está sendo executado. Agora há um relatório de resultados para mostrar quais ações específicas foram tomadas. Para obter mais informações, consulte Correção automática.
- **Suporte à linha de comando.** O Cloud Health Check agora pode ser executado a partir da linha de comando. Para obter mais informações, consulte Executando o Cloud Health Check na linha de comando.
- **Status do driver de injeção universal Citrix™.** O Cloud Health Check agora mostra o status do driver Citrix UVI e tem uma verificação de log de eventos relacionada para drivers Citrix UVI.
- **Verificação do registro de inicialização da sessão.** O Cloud Health Check agora verifica as configurações do registro de inicialização da sessão.
- **Atualizações no relatório de verificação.** Para itens verificados que possuem vários pontos de verificação, o relatório de verificação final agora lista todas as verificações que foram verificadas para mostrar quais ações foram realizadas durante a verificação de integridade.

Para obter mais informações, consulte Cloud Health Check.

Solucione problemas de registro de VDA e inicialização de sessão usando a Configuração Completa. Usando a interface de gerenciamento de Configuração Completa, agora você pode executar verificações que avaliam a integridade dos VDAs. As verificações de integridade do VDA identificam possíveis causas para problemas comuns de registro de VDA e inicialização de

sessão. Você pode executar verificações de integridade individualmente e em lotes. Para obter mais informações, consulte Verificações de integridade do VDA.

Capacidade de especificar a data de expiração do segredo do Azure para conexões existentes. Usando a interface de gerenciamento de Configuração Completa, agora você pode especificar a data após a qual o segredo do aplicativo expira. Para obter orientação sobre como visualizar a data de expiração do segredo, consulte Ambientes de nuvem do Microsoft Azure Resource Manager. Ao usar este recurso, considere as seguintes diferenças:

- Para entidades de serviço criadas manualmente no Azure, você pode editar diretamente a data de expiração na página **Editar Conexão > Propriedades da Conexão**.
- Para edições pela primeira vez da data de expiração para entidades de serviço criadas por meio da Configuração Completa em seu nome, vá para **Editar Conexão > Editar configurações > Usar existente**. Você pode fazer edições subsequentes na página **Editar Conexão > Propriedades da Conexão**.

Um botão para adicionar administradores. Adicionamos um botão, **Adicionar Administrador**, à guia **Configuração Completa > Administradores > Administradores**. O botão oferece uma maneira rápida de ir para **Gerenciamento de Identidade e Acesso > Administradores**, onde você pode adicionar (convidar) administradores. Para obter mais informações, consulte Adicionar um administrador.

Novo visual e experiência dos assistentes na Configuração Completa. Atualizamos os assistentes nos seguintes nós com um novo estilo, incluindo cores, fontes e outras alterações de formatação, para proporcionar uma melhor experiência ao usuário: **Administradores**, **Hospedagem**, **StoreFront**, **Pacotes de Aplicativos**, **Zonas** e **Configurações**. Os novos assistentes aparecem em visualizações de lâmina com viewports mais amplos, permitindo a exibição de mais conteúdo. Os fluxos de trabalho para configurar suas configurações permanecem os mesmos.

Suporte para retenção de disco do sistema quando o MCS I/O está habilitado para máquinas executadas no Google Cloud Platform (GCP). Na interface de gerenciamento de Configuração Completa, ao provisionar máquinas no GCP, agora você pode reter o disco do sistema durante os ciclos de energia quando a otimização de armazenamento do MCS (MCS I/O) estiver habilitada. Para obter mais informações, consulte Habilitando atualizações de otimização de armazenamento do MCS.

Suporte para upload ou download direto do EBS no Amazon Web Services (AWS). A AWS agora fornece API para permitir a criação direta de volume EBS com o conteúdo desejado. Agora você pode usar a API para eliminar a necessidade de um volume worker para a criação de

catálogos e adição de VMs. Para obter informações sobre as permissões da AWS necessárias para essa funcionalidade, consulte Ambientes de nuvem do Amazon Web Services.

Capacidade de identificar recursos do Amazon Web Services (AWS) criados pelo MCS. Adicionamos uma nova tag chamada `CitrixProvisioningSchemeID` para identificar recursos da AWS criados pelo MCS. Para obter mais informações, consulte Identificar recursos criados pelo MCS.

Capacidade de configurar o acesso a Gerenciar e Monitorar. A interface de gerenciamento de Configuração Completa agora oferece opções adicionais para controlar se as funções personalizadas terão acesso a **Gerenciar** e **Monitorar**. Para obter mais informações, consulte Criar e gerenciar funções.

Dezembro de 2021

Recursos novos e aprimorados

Suporte para Google Cloud VMware Engine. A plataforma agora permite migrar cargas de trabalho Citrix locais baseadas em VMware para o Google Cloud e seu ambiente principal do Citrix Virtual Apps and Desktops para o serviço Citrix Virtual Apps and Desktops. Para obter mais informações, consulte Suporte ao Google Cloud Platform (GCP) VMware Engine.

Capacidade de especificar com o que os nomes de conta começam ao especificar um esquema de nomenclatura. Esta versão introduz uma opção na página **Configuração do Catálogo de Máquinas > Identidades da Máquina** da interface de gerenciamento de Configuração Completa. A opção permite especificar números ou letras com os quais os nomes das contas começam, dando a você mais controle sobre como as contas de máquina são nomeadas durante a criação do catálogo. Para obter mais informações, consulte Identidades da máquina.

Suporte para criação de conexões Nutanix AHV XI e Nutanix AHV Prism Central (PC). Na interface de gerenciamento de Configuração Completa, agora você pode criar conexões Nutanix AHV XI e Nutanix AHV PC. Para obter mais informações, consulte Ambientes de virtualização Nutanix.

Suporte para seleção do tipo de armazenamento para discos de SO ao provisionar VMs no GCP. Na interface de gerenciamento de Configuração Completa, ao provisionar VMs no GCP, agora você pode selecionar o tipo de armazenamento para o disco do SO. As opções de armazenamento disponíveis na página **Configuração do Catálogo de Máquinas >**

Armazenamento incluem **Disco persistente padrão**, **Disco persistente balanceado** e **Disco persistente SSD**. Para obter mais informações, consulte Criar um catálogo de máquinas.

A interface de gerenciamento de Configuração Completa agora oferece suporte a disco efêmero do Azure. Anteriormente, o PowerShell era sua única opção para criar máquinas que usavam discos de SO efêmeros. Agora adicionamos uma opção, **Disco de SO efêmero do Azure**, à página **Configuração do Catálogo de Máquinas > Tipos de Armazenamento e Licença**. Selecione a opção se quiser usar o disco local da VM para hospedar o disco do sistema operacional. Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Proteger recursos gerenciados pelo Machine Creation Services (MCS) contra exclusão acidental. Agora você pode proteger os recursos gerenciados pelo MCS no Google Cloud Platform (GCP) aplicando o sinalizador `deletionProtection` do GCP habilitado para as VMs. Usando a permissão `compute.instances.setDeletionProtection` ou a função IAM Compute Admin, você pode redefinir o sinalizador para permitir que o recurso seja excluído. Essa funcionalidade é aplicável a catálogos persistentes e não persistentes. Para obter mais informações, consulte Proteger exclusão acidental de máquina.

Novembro de 2021

Recursos novos e aprimorados

Anotar uma imagem ao atualizar máquinas. Na interface de gerenciamento de Configuração Completa, agora você pode anotar uma imagem adicionando uma nota para ela ao atualizar um catálogo criado pelo MCS. Cada vez que você atualiza o catálogo, uma entrada relacionada à nota é criada, independentemente de você adicionar uma nota. Se você atualizar o catálogo sem adicionar uma nota, a entrada aparecerá como nula (-). Para visualizar o histórico de notas da imagem, selecione o catálogo, clique em **Propriedades do Modelo** no painel inferior e, em seguida, clique em **Visualizar histórico de notas**. Para obter mais informações, consulte Atualizar um catálogo.

Suporte a licenciamento multi-tipo. A interface de gerenciamento de Configuração Completa agora oferece suporte a licenciamento multi-tipo, permitindo que você especifique qual direito de licença você deseja que seu site (sua implantação de um produto de serviço Citrix Virtual Apps and Desktops) ou um grupo de entrega use.

- No nível do site, você determina qual licença usar em todo o site quando os usuários iniciam um aplicativo ou uma área de trabalho em seus dispositivos. A licença selecionada se aplica a todos os grupos de entrega, exceto aqueles configurados com uma licença diferente.

- No nível do grupo de entrega, você determina qual licença deseja que o grupo de entrega use, aproveitando a flexibilidade e os benefícios do licenciamento multi-tipo.

Para obter mais informações, consulte Licenças.

Suporte para exibir informações do plano de compra do Azure Marketplace. Na interface de gerenciamento de Configuração Completa, ao criar um catálogo de máquinas, agora você pode visualizar as informações do plano de compra para imagens mestras originadas de imagens do Azure Marketplace.

Outubro de 2021

Recursos novos e aprimorados

Capacidade de atualizar catálogos MCS persistentes. Introduzimos a opção **Atualizar Máquinas** para catálogos MCS persistentes na interface de gerenciamento de Configuração Completa. A opção permite gerenciar a imagem ou o modelo que o catálogo usa. Ao atualizar um catálogo persistente, considere o seguinte: Somente as máquinas que você adicionar ao catálogo posteriormente serão criadas usando a nova imagem ou modelo. Não implementamos a atualização para máquinas existentes no catálogo. Para obter mais informações, consulte Atualizar um catálogo.

Opção para provisionar VMs em um host dedicado do Azure. Adicionamos uma opção, **Usar um grupo de hosts**, à página **Configuração do Catálogo de Máquinas > Imagem Mestra** da interface de gerenciamento de Configuração Completa. A opção permite especificar qual grupo de hosts você deseja usar ao provisionar VMs em ambientes Azure. Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Melhorar o desempenho preservando uma VM provisionada durante o ciclo de energia. Adicionamos uma configuração, **Reter VMs entre ciclos de energia**, à página **Configuração do Catálogo de Máquinas > Configurações de Disco** da interface de gerenciamento de Configuração Completa. A configuração permite preservar uma VM provisionada durante o ciclo de energia em ambientes Azure. Para obter mais informações, consulte Otimização de armazenamento MCS. Alternativamente, você pode configurar o recurso usando o PowerShell. Para obter mais informações, consulte Preservando uma máquina virtual provisionada durante o ciclo de energia.

Vincular um catálogo de máquinas a um conjunto de configuração do Workspace Environment Management. Ao criar um catálogo de máquinas, agora você pode vinculá-lo a um conjunto de configuração do Workspace Environment Management. Isso permite que você use o serviço Workspace Environment Management para oferecer a melhor experiência de espaço de

trabalho possível aos seus usuários. Você também pode optar por vincular o catálogo depois de criá-lo. Para obter mais informações, consulte Criar catálogos de máquinas e Gerenciar catálogos de máquinas.

Setembro de 2021

Recursos novos e aprimorados

Adicionar descrição informativa para atualizações de imagem. Agora você pode adicionar descrições informativas sobre alterações relacionadas a atualizações de imagem para catálogos de máquinas. Essa funcionalidade é útil para administradores que desejam adicionar rótulos descritivos ao atualizar uma imagem usada por um catálogo, por exemplo, *Office 365 instalado*. Usando comandos PowerShell, você pode criar e visualizar essas mensagens. Para obter detalhes, consulte Adicionar descrições a uma imagem.

Integração com o Azure VMware Solution (AVS). O serviço Citrix Virtual Apps and Desktops oferece suporte ao AVS, o Azure VMware Solution. O AVS fornece infraestrutura de nuvem contendo clusters vSphere criados pelo Azure. Aproveite o serviço Citrix Virtual Apps and Desktops para usar o AVS para provisionar sua carga de trabalho VDA da mesma forma que você usaria o vSphere em ambientes locais. Para obter mais informações, consulte Integração do Azure VMware Solution.

Mesmo grupo de recursos para vários catálogos. Agora você pode usar o mesmo grupo de recursos para atualizar e criar catálogos no serviço Citrix Virtual Apps and Desktops. Este processo:

- aplica-se a qualquer grupo de recursos que contenha um ou mais catálogos de máquinas.
- suporta grupos de recursos que não são criados pelo Machine Creation Services.
- cria a VM e os recursos associados.
- exclui recursos no grupo de recursos quando a VM ou o catálogo é removido.

Para obter mais informações, consulte Grupos de recursos do Azure.

Recuperar informações para VMs do Azure, instantâneos, disco do SO e definição de imagem da galeria. Você pode exibir informações para uma VM do Azure, disco do SO, instantâneo e definição de imagem da galeria. Essas informações são exibidas para recursos na imagem mestre quando um catálogo de máquinas é atribuído. Use essa funcionalidade para visualizar e selecionar uma imagem Linux ou Windows. Para obter mais informações, consulte

Recuperar informações para VMs do Azure, instantâneos, disco do SO e definição de imagem da galeria.

Nova atualização para Configuração Automatizada. A Configuração Automatizada foi atualizada para uma nova versão com recursos que incluem:

- Suporte a Machine Creation Services (MCS) - A Configuração Automatizada agora oferece suporte a catálogos MCS. Para obter mais informações, consulte Compreendendo a migração de catálogos provisionados pelo Machine Creation Services.

Outras atualizações para a Configuração Automatizada incluem:

- Suporte a Zonas aprimorado pré-preenchendo o arquivo ZoneMapping.yml com os nomes das zonas locais durante a exportação e os Locais de Recursos da nuvem durante o backup.
- O StoreFront foi transformado em um componente gerenciável de nível superior. Antes disso, o StoreFront era gerenciado como parte dos Grupos de Entrega. Essa separação facilita melhor a fusão de sites.
- Alterado `AddMachinesOnly` para `MergeMachines` para corresponder ao padrão das opções de mesclagem atuais e novas.
- Adicionado o uso do arquivo SecurityClient.csv para importar o ClientId e o Secret ao criar e atualizar o CustomerInfo.yml ao usar os cmdlets de suporte.
- Adicionada a migração de Preferências de Zona do Usuário.
- Suporte corrigido para o Plano de Controle japonês.
- Outras correções e melhorias.

Baixe a Configuração Automatizada em Downloads da Citrix. Para obter mais informações sobre a Configuração Automatizada, consulte Migrar configuração para o Citrix Cloud.

Mais opções de agendamento disponíveis com agendamentos de reinicialização. A interface de gerenciamento de Configuração Completa agora oferece opções adicionais para controlar quando as reinicializações agendadas ocorrem. Além dos agendamentos de reinicialização diários recorrentes, agora você pode definir padrões de recorrência semanais e mensais. Para obter mais informações, consulte Criar um agendamento de reinicialização.

Preservar colunas personalizadas que degradam o desempenho. Anteriormente, no nó **Pesquisar** da interface de gerenciamento de Configuração Completa, as colunas personalizadas que degradavam o desempenho desapareciam depois que você atualizava a janela do navegador ou saía do console e fazia login novamente. Agora você pode controlar se deseja preservar essas

colunas personalizadas. Para obter mais informações, consulte Usar Pesquisa na interface de gerenciamento de Configuração Completa.

Use a ferramenta de Configuração Automatizada para fazer backup e restaurar. Adicionamos um nó, **Backup e Restauração**, à interface de gerenciamento de Configuração Completa. Esse nó agrega todos os recursos relacionados à ferramenta de Configuração Automatizada, incluindo informações sobre:

- Agendamento de backups automatizados da sua configuração do Citrix Virtual Apps and Desktops usando um único comando
- Restauração de um backup anterior, se necessário
- Execução de backups e restaurações de forma granular
- Outros casos de uso suportados

Para obter mais informações, consulte a documentação de Configuração Automatizada.

Suporte para catálogos não associados a domínio. Adicionamos um tipo de identidade, **Não associado a domínio**, à página **Configuração do Catálogo de Máquinas > Identidades de Máquina** da interface de gerenciamento de Configuração Completa. Com esse tipo de identidade, você pode usar o MCS para criar máquinas que não estão associadas a nenhum domínio. Para obter mais informações, consulte Criar catálogos de máquinas.

Suporte para usar um perfil de máquina. Adicionamos uma opção, **Usar um perfil de máquina**, à página **Configuração do Catálogo de Máquinas > Imagem Mestra** da interface de gerenciamento de Configuração Completa. A opção permite especificar qual perfil de máquina você deseja que as VMs herdem as configurações ao criar VMs em ambientes Azure. As VMs no catálogo podem então herdar configurações do perfil de máquina selecionado. Exemplos de configurações incluem:

- Rede acelerada
- Diagnóstico de inicialização
- Cache de disco do host (relacionado a discos de SO e MCSIO)
- Tamanho da máquina (salvo especificação em contrário)
- Tags colocadas na VM

Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Suporte para Windows Server 2022. Requer VDA 2106 mínimo.

Agosto de 2021

Recursos novos e aprimorados

Estender o número de itens classificáveis de 500 para 5.000. No nó **Pesquisar** da interface de gerenciamento de Configuração Completa, agora você pode classificar até 5.000 itens por qualquer cabeçalho de coluna. Quando o número de itens exceder 5.000, use filtros para reduzir o número de itens para 5.000 ou menos para permitir a classificação. Para obter mais informações, consulte Usar Pesquisa na interface de gerenciamento de Configuração Completa.

Suporte para tipos de armazenamento adicionais do Azure. Agora você pode selecionar diferentes tipos de armazenamento para máquinas virtuais em ambientes Azure usando MCS. Para obter detalhes, consulte Tipos de armazenamento.

Suporte para seleção do tipo de armazenamento para discos de cache de write-back. Na interface de gerenciamento de Configuração Completa, ao criar um catálogo MCS, agora você pode selecionar o tipo de armazenamento para o disco de cache de write-back. Os tipos de armazenamento disponíveis incluem: SSD Premium, SSD Padrão e HDD Padrão. Para obter mais informações, consulte Criar catálogos de máquinas.

Desligar máquinas suspensas. Na interface **Gerenciar > Configuração Completa**, adicionamos uma opção, **Quando não houver reconexão em (minutos)**, à página **Configurações baseadas em carga** da interface de usuário do Gerenciar Autoscale para grupos de entrega de SO de sessão única. A opção fica disponível depois que você seleciona **Suspender**, permitindo que você especifique quando desligar as máquinas suspensas. As máquinas suspensas permanecem disponíveis para usuários desconectados quando eles se reconectam, mas não estão disponíveis para novos usuários. Desligar as máquinas as torna disponíveis novamente para manipular todas as cargas de trabalho. Para obter mais informações, consulte Autoscale.

Suporte estendido para usar arquivos CSV para adicionar máquinas em massa a um catálogo. Na interface **Gerenciar > Configuração Completa**, agora você pode usar um arquivo CSV para adicionar em massa máquinas já existentes em seu data center a um catálogo onde essas máquinas são gerenciadas por energia. Para obter mais informações, consulte Criar catálogos de máquinas e Gerenciar catálogos de máquinas.

Julho de 2021

Recursos novos e aprimorados

Registro de configuração. A interface de usuário de **Registro** foi alterada em **Gerenciar > Configuração Completa**. As três guias a seguir compõem a interface:

- **Eventos** (anteriormente, registro de configuração). Esta guia permite rastrear alterações de configuração e atividades administrativas.
- **Tarefas**. Esta guia permite visualizar tarefas relacionadas a operações de catálogo de máquinas.
- **APIs**. Esta guia permite visualizar solicitações de API REST feitas durante um determinado período.

Para obter mais informações, consulte Registro de configuração.

O Autoscale agora oferece opções dinâmicas de tempo limite de sessão. Você pode configurar tempos limite de sessão desconectada e ociosa para seus horários de pico e fora de pico para obter um esvaziamento mais rápido da máquina e economia de custos. Para obter mais informações, consulte Tempos limite de sessão dinâmicos.

Suporte para Chaves de Criptografia Gerenciadas pelo Cliente (CMEK) do Google Cloud Platform (GCP). Agora você pode usar o CMEK do Google com catálogos MCS. O CMEK oferece maior controle sobre as chaves usadas para criptografar dados em um projeto do Google Cloud. Para obter mais informações, consulte Chaves de criptografia gerenciadas pelo cliente (CMEK). Para configurar este recurso, consulte Usando Chaves de Criptografia Gerenciadas pelo Cliente (CMEK). O recurso está disponível na página **Configuração do Catálogo de Máquinas > Configurações de Disco** da interface **Gerenciar > Configuração Completa**.

> **Nota:**
>
> Este recurso está disponível como uma prévia.

> **Atualizações na guia Gerenciar**. Atualizamos as opções no menu da guia **Gerenciar**:

- **Configuração Completa**: Anteriormente, esta opção levava você ao console legado. Agora, ela leva você ao novo console baseado na web (Web Studio). O console baseado na web tem paridade total com o console legado e inclui várias melhorias. Recomendamos que você comece a usá-lo agora.
- **Configuração Legada**: Esta opção leva você ao console legado, que está programado para ser removido em setembro de 2021. Depois disso, **Configuração Completa** será a única interface que oferece acesso a toda a gama de ações de configuração e gerenciamento.

O Web Studio agora oferece suporte à escolha de uma conexão de gerenciamento de energia para um catálogo de Acesso Remoto a PC. Anteriormente, você podia usar o Studio

para criar uma conexão de host Wake on LAN para seu local de recurso (selecionando **Remote PC Wake on LAN** como o tipo de conexão). No entanto, o PowerShell era sua única opção para associar essa conexão a um catálogo de Acesso Remoto a PC. Agora você pode usar o Studio para conseguir isso. Para obter mais informações, consulte Configurar Wake on LAN na interface de Configuração Completa.

Junho de 2021

Recursos novos e aprimorados

Acessar imagens da Galeria de Imagens Compartilhadas do Azure. Ao criar um catálogo de máquinas, agora você pode acessar imagens da Galeria de Imagens Compartilhadas do Azure na tela Imagem Mestra. Para obter detalhes, consulte Acessar imagens da Galeria de Imagens Compartilhadas do Azure.

Suporte a máquinas virtuais blindadas no Google Cloud Platform (GCP). Você pode provisionar máquinas virtuais blindadas no GCP. Uma máquina virtual blindada é reforçada por um conjunto de controles de segurança que fornecem integridade verificável de suas instâncias do Compute Engine, usando recursos avançados de segurança da plataforma, como inicialização segura, um módulo de plataforma confiável virtual, firmware UEFI e monitoramento de integridade. Para obter mais informações, consulte VMs blindadas.

Impor HTTPS ou HTTP. Use as configurações do registro para impor tráfego HTTPS ou HTTP por meio do serviço XML.

Sempre use SSD padrão para um disco de identidade para reduzir custos em ambientes Azure. Os catálogos de máquinas usam o tipo de armazenamento SSD padrão para discos de identidade. Os SSDs padrão do Azure são uma opção de armazenamento econômica otimizada para cargas de trabalho que precisam de desempenho consistente em níveis de IOPS mais baixos. Para obter mais informações sobre tipos de armazenamento, consulte Imagem mestre do Azure Resource Manager.

> **Nota:**
>
> Para obter mais informações sobre os preços de discos gerenciados do Azure, consulte Preços de discos gerenciados.

> **Novo recurso disponível no Web Studio**. Os seguintes recursos agora estão disponíveis no console baseado na web:

- **O Studio agora oferece suporte à autenticação no Azure para criar uma entidade de serviço**. Agora você pode estabelecer uma conexão de host com o Azure autenticando-se no Azure para criar uma entidade de serviço. Esse suporte elimina a necessidade de criar manualmente uma entidade de serviço em sua assinatura do Azure antes de criar uma conexão no Studio. Para obter mais informações, consulte Ambientes de virtualização do Microsoft Azure Resource Manager.
- **O Studio agora oferece suporte à clonagem de catálogos de máquinas existentes**. Esse recurso permite clonar um catálogo de máquinas existente para usar como modelo para um novo, eliminando a necessidade de criar um catálogo semelhante do zero. Ao clonar um catálogo, você não pode alterar as configurações associadas ao sistema operacional e ao gerenciamento de máquinas. O catálogo clonado herda essas configurações do original. Para obter mais informações, consulte Clonar um catálogo.
- **Um novo nó chamado Configurações agora disponível no painel de navegação do Studio**. O nó **Configurações** permite configurar as configurações que se aplicam a todo o site (sua implantação de um produto de serviço Citrix Virtual Apps and Desktops). As seguintes configurações estão disponíveis:

  - **Balancear carga de catálogos de várias sessões**. Selecione a opção de balanceamento de carga que atenda às suas necessidades. Essa configuração se aplica a todos os seus catálogos. Anteriormente, você acessava esse recurso clicando no ícone de engrenagem no canto superior direito do console. Para obter mais informações, consulte Balancear carga de máquinas.

- **Experiência de pesquisa aprimorada no Studio**. Esta versão aprimora sua experiência de pesquisa no Studio. Ao usar filtros para realizar uma pesquisa avançada, a janela Adicionar filtros aparece em primeiro plano, deixando a exibição em segundo plano inalterada. Para obter mais informações, consulte Usar Pesquisa na interface de gerenciamento de Configuração Completa.
- **Capacidade de suspender e retomar VMs do Google Cloud no MCS**. Agora você pode suspender e retomar VMs do Google Cloud no MCS como faria com qualquer VM. Para obter detalhes, consulte Gerenciar grupos de entrega. Para habilitar essa capacidade, defina as permissões `compute.instances.suspend` e `compute.instances.resume` na conta de serviço do Google Cloud. A função de Administrador de Computação vem com essas permissões.

  No Citrix Virtual Apps and Desktops, você também pode usar o comando PowerShell `New-BrokerHostingPowerAction` para suspender e retomar as VMs. Para obter detalhes, consulte New-Brokerhostingpoweraction.

O Google Cloud impõe algumas limitações sobre o tipo e a configuração das instâncias que podem ser suspensas. Para obter informações adicionais, consulte Suspensão e retomada de uma instância no site do Google Cloud.

Maio de 2021

Recursos novos e aprimorados

Reconexão de sessão após desconexão da máquina em modo de manutenção. Anteriormente, quando usuários de desktop (VDI) de sessão única agrupados (aleatórios) eram desconectados de uma máquina em modo de manutenção, a reconexão da sessão não era permitida a nenhuma máquina no pool. Máquinas de sessão múltipla e de sessão única estática sempre permitiam a reconexão da sessão nessa circunstância.

Agora, usando o PowerShell, você pode controlar no nível do grupo de entrega se a reconexão da sessão é permitida após uma desconexão ocorrer em uma máquina em modo de manutenção. Isso se aplica a todos os VDAs no grupo (sessão única e sessão múltipla).

Para obter detalhes, consulte Controlar a reconexão da sessão quando desconectado da máquina em modo de manutenção.

Suporte a sondagem de aplicativos e sondagem de desktops em todas as edições do Citrix Virtual Apps and Desktops Service. Além do suporte existente da edição **Premium**, a sondagem de aplicativos e a sondagem de desktops agora estão disponíveis nas edições **Citrix Virtual Apps Advanced Service** e **Citrix Virtual Apps and Desktops Advanced Service**.

Novo recurso disponível no Web Studio. O seguinte recurso agora está disponível no console baseado na web:

- **O Studio agora oferece suporte à seleção de Zonas de Disponibilidade do Azure**. Anteriormente, o PowerShell era sua única opção para provisionar máquinas em uma Zona de Disponibilidade específica em ambientes Azure. Ao usar o Studio para criar um catálogo de máquinas, agora você pode selecionar uma ou mais Zonas de Disponibilidade nas quais deseja provisionar máquinas. Se nenhuma zona for especificada, o Machine Creation Services (MCS) permite que o Azure coloque as máquinas dentro da região. Se mais de uma zona for especificada, o MCS distribui aleatoriamente as máquinas entre elas. Para obter mais informações, consulte Provisionar máquinas em zonas de disponibilidade especificadas.

Disco efêmero do Azure. O serviço Citrix Virtual Apps and Desktops oferece suporte ao disco efêmero do Azure. Um disco efêmero permite que você reutilize o disco de cache para armazenar o disco do sistema operacional para uma máquina virtual habilitada para Azure. Essa

funcionalidade é útil para ambientes Azure que exigem um disco SSD de maior desempenho em vez de um disco HDD padrão.

> **Nota:**
>
> Catálogos persistentes não suportam discos de SO efêmeros. Além disso, ao usar este recurso, considere que o disco de desempenho extra incorre em um custo adicional. É benéfico reutilizar o disco de cache para armazenar o disco do SO em vez de pagar por um disco gerenciado extra.

> Discos de SO efêmeros exigem que seu esquema de provisionamento use discos gerenciados e uma Galeria de Imagens Compartilhadas. Para obter mais informações, consulte Discos efêmeros do Azure.

Desempenho aprimorado para VDAs gerenciados por MCS no Azure. O serviço Citrix Virtual Apps and Desktops melhora o desempenho para VDAs gerenciados com Machine Creation Services (MCS) no Azure. Este aprimoramento altera os valores padrão para *Ações Simultâneas Absolutas* para a conexão de hospedagem para 500, e *Máximo de novas ações por minuto* para a conexão de hospedagem para 2.000. Nenhuma tarefa de configuração manual é necessária para aproveitar este aprimoramento. Para obter detalhes, consulte Limitação do Azure.

Novos recursos disponíveis no Cloud Health Check. O Cloud Health Check foi atualizado para uma nova versão com recursos que incluem:

- **Descoberta automática de máquinas VDA**. O Cloud Health Check agora pode descobrir e recuperar automaticamente VDAs de suas implantações do serviço Citrix Virtual Apps and Desktops. Para obter mais informações, consulte Recuperar máquinas VDA.
- **Agendamento de verificações de integridade**. O Cloud Health Check agora permite que você configure agendamentos para realizar verificações de integridade periódicas. Para obter mais informações, consulte Agendador do Cloud Health Check.
- **Informações da versão do Cloud Health Check**. Agora você pode verificar qual versão do Cloud Health Check está usando. Para visualizar as informações da versão, clique no ícone de engrenagem no canto superior direito da janela principal do Cloud Health Check.
- **Correção automática**. O Cloud Health Check agora oferece suporte à detecção e correção automática de certos problemas identificados em máquinas onde ele está sendo executado. Para obter mais informações, consulte Correção automática.

> **Nota:**
>
> A correção automática está disponível como uma prévia.

Abril de 2021

Recursos novos e aprimorados

Recuperar instâncias dinâmicas usando a API da AWS. O serviço Citrix Virtual Apps and Desktops agora consulta a AWS para recuperar tipos de instância dinamicamente. Essa funcionalidade elimina a necessidade de criar um arquivo `InstanceTypes.xml` personalizado para os clientes que desejam usar tamanhos de máquina além dos definidos no serviço Citrix Virtual Apps and Desktops. Essas informações eram fornecidas anteriormente pelo arquivo `InstanceTypes.xml`. Para facilitar esse acesso dinâmico aos tipos de instância da AWS disponíveis, os usuários devem atualizar as permissões em seus principais de serviço para incluir permissões `ec2:DescribeInstanceTypes`. Para oferecer suporte à compatibilidade retroativa para clientes que optam por não atualizar suas permissões de principal de serviço, os tipos de instância da AWS listados em `InstanceTypes.xml` são usados. Esse processo gera uma mensagem de aviso para o log CDF do MCS.

> **Nota:**
>
> O Citrix Studio não exibe a mensagem de aviso contida no log CDF.

> Para obter mais informações sobre permissões, consulte Definindo permissões IAM e Sobre permissões AWS.

Novo recurso disponível no Web Studio. O seguinte recurso agora está disponível no console baseado na web:

- **O Studio agora exibe a data e a hora do seu fuso horário**. Anteriormente, o Studio exibia apenas a data e a hora com base no relógio e fuso horário do sistema. O Studio agora oferece suporte à exibição de data e hora locais ao seu fuso horário quando você passa o ponteiro do mouse sobre um item de evento. A hora é expressa em UTC.

Suporte de E/S do MCS para VMs do Azure sem armazenamento temporário. O MCS I/O agora oferece suporte à criação de catálogo de máquinas para VMs que não possuem discos temporários ou armazenamento anexado. Com este suporte:

- O snapshot (disco gerenciado) é recuperado da VM de origem *sem* armazenamento temporário. As VMs no catálogo de máquinas não possuem armazenamento temporário.
- O snapshot (disco gerenciado) é recuperado da VM de origem *com* armazenamento temporário. As VMs no catálogo de máquinas possuem armazenamento temporário.

Para obter mais informações, consulte Otimização de armazenamento do Machine Creation Services (MCS)

Novo recurso disponível no Web Studio. O seguinte recurso agora está disponível no console baseado na web:

- **Forçar logoff**. O Autoscale agora permite que você faça logoff de sessões existentes em máquinas à força quando o período de carência estabelecido for atingido, tornando a máquina elegível para desligamento. Isso permite que o Autoscale desligue as máquinas muito mais rapidamente, reduzindo assim os custos. Você pode enviar notificações aos usuários antes que eles sejam desconectados. Para obter mais informações, consulte Autoscale.

Nova atualização para Configuração Automatizada. A Configuração Automatizada foi atualizada para uma nova versão com recursos que incluem:

- **Mesclar vários sites** – você pode mesclar vários sites em um único site, evitando colisões de nomes usando prefixos e sufixos. Para obter mais informações, consulte Mesclar vários sites em um único site.
- **Ativação de site** – você pode selecionar se sua implantação local ou na nuvem controla recursos como agendamentos de reinicialização e esquemas de energia. Para obter mais informações, consulte Ativar sites.

Outras atualizações para a Configuração Automatizada incluem:

- A capacidade de migrar funções e escopos de administrador.
- Um parâmetro `Quiet` para selecionar cmdlets para suprimir o registro em log do console.
- Um parâmetro `SecurityFileFolder` para permitir a colocação do arquivo CvadAcSecurity.yml em um compartilhamento de arquivo de rede seguro que requer autenticação.
- A capacidade de filtrar por nome de máquina em catálogos de máquinas e grupos de entrega.

- Melhorias nos parâmetros de seleção de componentes para usar o método de parâmetro de alternância, eliminando a necessidade de adicionar um `$true` após o nome do componente.
- Um novo cmdlet (`New-CvadAcZipInfoForSupport`) para compactar todos os seus arquivos de log para enviar à Citrix para suporte.

Baixe a Configuração Automatizada em Downloads da Citrix. Para obter mais informações sobre a Configuração Automatizada, consulte Migrando para a nuvem.

Preservar instâncias do GCP em ciclos de energia. As instâncias não persistentes do Google Cloud Platform (GCP) não são mais excluídas ao serem desligadas. Em vez disso, as instâncias são preservadas em ciclos de energia. Quando uma instância não persistente é desligada, o disco do SO é desanexado e excluído. Quando a instância é ligada, o disco do SO é recriado a partir do disco base e anexado à instância existente.

Suporte para imagens Azure Gen2. Agora você pode provisionar um catálogo de VMs Gen2 usando um snapshot Gen2 ou um disco gerenciado Gen2 para melhorar o desempenho do tempo de inicialização. Para obter mais informações, consulte Criar catálogos de máquinas. Os seguintes sistemas operacionais são suportados para imagens Azure Gen2:

- Windows Server 2019, 2016, 2012 e 2012 R2
- Windows 10

> **Nota:**
>
> A criação de um catálogo de máquinas Gen2 usando um snapshot Gen1, ou disco gerenciado, não é suportada. Da mesma forma, a criação de um catálogo de máquinas Gen1 usando um snapshot Gen2, ou disco gerenciado, também não é suportada. Para obter mais informações, consulte Suporte para VMs de geração 2 no Azure.

> **Desativando contas de armazenamento de tabela**. O Machine Creation Services (MCS) não cria mais contas de armazenamento de tabela para catálogos que usam discos gerenciados ao provisionar VDAs no Azure. Para obter mais informações, consulte Armazenamento de tabela do Azure.

Eliminando bloqueios em contas de armazenamento. Ao criar um catálogo no Azure usando um disco gerenciado, uma conta de armazenamento não é mais criada. As contas de armazenamento criadas para catálogos existentes permanecem inalteradas. Essa alteração é aplicável apenas a discos gerenciados. Para discos não gerenciados, não há alteração no

comportamento existente. O Machine Creation Services (MCS) continua criando contas de armazenamento e bloqueios.

Novos recursos disponíveis no Web Studio. Os seguintes recursos estão agora disponíveis no console baseado na web:

- **Use uma chave de criptografia gerenciada pelo cliente para criptografar dados em máquinas**. O Studio agora adiciona uma configuração chamada **Chave de criptografia gerenciada pelo cliente** à página **Configuração do Catálogo de Máquinas > Configurações de Disco**. A configuração permite que você escolha se deseja criptografar dados nas máquinas a serem provisionadas no catálogo. Para obter mais informações, consulte Chave de criptografia gerenciada pelo cliente.
- **O Studio agora oferece suporte à restrição do Autoscale a máquinas marcadas**. Anteriormente, você precisava usar o PowerShell para restringir o Autoscale a certas máquinas em um grupo de entrega. Agora você também pode usar o Studio. Para obter mais informações, consulte Restringir o Autoscale a certas máquinas em um grupo de entrega.

Março de 2021

Recursos novos e aprimorados

Hosts dedicados do Azure. Os hosts dedicados do Azure permitem provisionar máquinas virtuais em hardware dedicado a um único cliente. Ao usar um host dedicado, o Azure garante que suas máquinas virtuais seriam as únicas máquinas em execução nesse host. Isso oferece mais controle e visibilidade aos clientes, garantindo que eles atendam aos seus requisitos regulatórios ou de segurança interna. Um grupo de host do Azure pré-configurado, na região da unidade de hospedagem, é necessário ao usar o parâmetro `HostGroupId`. Além disso, o posicionamento automático do Azure é necessário. Para obter mais informações, consulte Hosts dedicados do Azure.

> **Dica:**

> Ao usar hosts dedicados do Azure, a seleção da **Zona de Disponibilidade do Azure** não tem efeito. A máquina virtual é colocada pelo processo de posicionamento automático do Azure.

> **Suporte para criptografia do lado do servidor do Azure**. O serviço Citrix Virtual Apps and Desktops oferece suporte a chaves de criptografia gerenciadas pelo cliente para discos gerenciados do Azure. Com esse suporte, você pode gerenciar seus requisitos organizacionais e de conformidade criptografando os discos gerenciados do seu catálogo de máquinas usando sua própria chave de criptografia. Para obter mais informações, consulte Criptografia do lado do servidor do Azure.

Provisionar máquinas em zonas de disponibilidade especificadas no Azure. Agora você pode provisionar máquinas em uma zona de disponibilidade específica em ambientes Azure. Com essa funcionalidade:

- Você pode especificar uma ou várias Zonas de Disponibilidade no Azure. As máquinas são nominalmente distribuídas igualmente por todas as zonas fornecidas, se mais de uma zona for fornecida.
- A máquina virtual e o disco correspondente são colocados na zona (ou zonas) especificada.
- Você pode navegar pelas Zonas de Disponibilidade para uma determinada oferta de serviço ou região. As Zonas de Disponibilidade válidas são exibidas usando comandos PowerShell. Visualize os itens de inventário da oferta de serviço usando `Get-Item`.

Para obter mais informações, consulte Provisionar máquinas em zonas de disponibilidade especificadas no Azure.

Novos recursos disponíveis no Web Studio. Os seguintes recursos estão agora disponíveis no console baseado na web:

- **O Studio agora oferece suporte à associação de aplicativos com ícones personalizados**. Anteriormente, você precisava usar o PowerShell para adicionar ícones personalizados para uso com aplicativos publicados. Agora você também pode usar o Studio para fazer isso. Para obter mais informações, consulte Gerenciar grupos de aplicativos.
- **O Studio agora oferece suporte à aplicação de tags a catálogos de máquinas**. Anteriormente, você poderia usar o Studio para criar ou excluir tags para uso com um catálogo. No entanto, você precisava usar o PowerShell para aplicar tags ao catálogo. Agora você também pode usar o Studio para aplicar ou remover uma tag de um catálogo, assim como faz com grupos de entrega. Para obter mais informações, consulte Aplicar tags a catálogos de máquinas.
- **O Studio agora oferece suporte à alternância entre os modos "balanceamento de carga horizontal" e "balanceamento de carga vertical"**. Anteriormente, o PowerShell era sua única opção para alternar entre os modos de balanceamento de carga horizontal e vertical. O

Studio agora oferece mais flexibilidade para controlar como balancear a carga de máquinas de SO multi-sessão. Para obter mais informações, consulte Balancear carga de máquinas.

- **O Studio agora oferece suporte à inclusão de máquinas em modo de manutenção em agendamentos de reinicialização**. Anteriormente, o PowerShell era sua única opção para configurar reinicializações agendadas para máquinas em modo de manutenção. Agora você também pode usar o Studio para controlar se essas máquinas devem ser incluídas em um agendamento de reinicialização. Para obter mais informações, consulte Criar um agendamento de reinicialização.
- **O Studio agora oferece suporte à configuração de Wake on LAN para Acesso Remoto a PC**. Anteriormente, você precisava usar o PowerShell para configurar o Wake on LAN para Acesso Remoto a PC. Agora você também pode usar o Studio para configurar o recurso. Para obter mais informações, consulte Configurar Wake on LAN.
- **O Studio agora oferece suporte à aplicação de propriedades de instância AWS e à marcação de recursos operacionais**. Ao criar um catálogo para provisionar máquinas na AWS usando o MCS, você pode especificar se deseja aplicar a função IAM e as propriedades de tag a essas máquinas. Você também pode especificar se deseja aplicar tags de máquina a recursos operacionais. Você tem as duas opções a seguir:
  - **Aplicar propriedades de modelo de máquina a máquinas virtuais**
  - **Aplicar tags de máquina a recursos operacionais**

  Para mais informações, consulte Aplicando propriedades de instância AWS e marcando recursos operacionais.

Galeria de Imagens Compartilhadas do Azure. O serviço Citrix Virtual Apps and Desktops oferece suporte à Galeria de Imagens Compartilhadas do Azure como um repositório de imagens publicado para máquinas provisionadas por MCS no Azure. Os administradores têm a opção de armazenar uma imagem na galeria para acelerar a criação e a hidratação de discos de SO. Esse processo melhora os tempos de inicialização e de lançamento de aplicativos para VMs não persistentes. Para obter detalhes sobre esse recurso, consulte Galeria de imagens compartilhadas do Azure.

> **Nota:**
>
> A funcionalidade da Galeria de Imagens Compartilhadas é compatível com discos gerenciados. Não está disponível para catálogos de máquinas legados.

Buckets de armazenamento criados na mesma região do Google Cloud Platform que o catálogo de máquinas. Em versões anteriores, o MCS criava buckets de armazenamento temporários durante o provisionamento como parte do processo de upload de disco. Esses buckets abrangiam várias regiões, que o Google define como uma grande área geográfica contendo dois ou mais locais geográficos. Esses buckets temporários residiam na localização geográfica dos Estados Unidos, independentemente de onde o catálogo fosse provisionado. O MCS agora cria buckets de armazenamento na mesma região onde você provisiona seus catálogos. Os buckets de armazenamento não são mais temporários; eles permanecem em seu projeto do Google Cloud Platform após a conclusão do processo de provisionamento. Futuras operações de provisionamento usarão o bucket de armazenamento existente, se houver um nessa região. Um novo bucket de armazenamento será criado se não houver um na região especificada.

Fevereiro de 2021

Recursos novos e aprimorados

Suporte para imagens Gen2 do Azure. Agora você pode provisionar discos gerenciados usando VMs Gen2 em ambientes Azure para melhorar o desempenho do tempo de inicialização. Os seguintes sistemas operacionais são suportados:

- Windows Server 2019, 2016, 2012 e 2012 R2
- Windows 10

Nota:

Com este suporte, apenas um subconjunto de VMs é suportado. Por exemplo, algumas VMs podem ser dos tipos Gen1 e Gen2, enquanto outras VMs podem ser apenas Gen1. Para obter mais informações, consulte Suporte para VMs de geração 2 no Azure.

Agendamentos de reinicialização de máquina. O Citrix Studio agora adiciona uma opção chamada **Reiniciar todas as máquinas após o esgotamento das sessões** ao menu **Duração da reinicialização**. A opção permite que você escolha se deseja reiniciar todas as máquinas após o esgotamento de todas as sessões. Quando o tempo de reinicialização é atingido, as máquinas são colocadas no estado de esgotamento e reiniciadas quando todas as sessões são encerradas. Para obter mais informações, consulte Criar um agendamento de reinicialização.

Novos recursos disponíveis no Web Studio. Os seguintes recursos estão agora disponíveis no console baseado na web:

- **O Studio agora oferece suporte ao uso de arquivos CSV para adicionar máquinas em massa a um catálogo**. Este recurso permite que você use um arquivo CSV para:
  - Adicionar máquinas em massa a um catálogo de SO de sessão múltipla ou sessão única onde as máquinas não são gerenciadas por energia através do Studio.
  - Adicionar máquinas em massa a um catálogo de Acesso Remoto a PC. Anteriormente, você tinha que escolher UOs para adicionar máquinas em massa a um catálogo de Acesso Remoto a PC. Fazer isso, no entanto, não é fácil em cenários com restrições de estrutura de UO. O recurso oferece mais flexibilidade para adicionar máquinas em massa. Você pode adicionar apenas máquinas (para uso com atribuições automáticas de usuário) ou adicionar máquinas juntamente com atribuições de usuário.

  Para obter mais informações, consulte Criar catálogos de máquinas e Gerenciar catálogos de máquinas.
- **Suporte estendido para Citrix Managed Azure.** Citrix Managed Azure agora está disponível nas seguintes edições do serviço Citrix Virtual Apps and Desktops: Standard for Azure, Advanced, Premium e Workspace Premium Plus.
- **Suporte para colocar imagens mestre na Galeria de Imagens Compartilhadas do Azure**. O Studio agora oferece uma opção para colocar imagens mestre na Galeria de Imagens Compartilhadas do Azure (SIG). A SIG é um repositório para gerenciar e compartilhar imagens. Ela permite que você disponibilize suas imagens em toda a sua organização. Recomendamos que você armazene uma imagem mestre na SIG ao criar grandes catálogos de máquinas não persistentes, pois isso permite uma redefinição mais rápida dos discos do SO VDA. Para obter mais informações, consulte Ambientes de virtualização do Microsoft Azure Resource Manager.
- **Manter disco do sistema para catálogos de máquinas MCS no Azure**. O Studio agora permite que você controle se deseja reter discos do sistema para VDAs durante os ciclos de energia. Normalmente, o disco do sistema é excluído no desligamento e recriado na inicialização. Isso garante que o disco esteja sempre em um estado limpo, mas resulta em tempos de reinicialização da VM mais longos. Se as gravações do sistema forem redirecionadas para o cache e gravadas de volta no disco de cache, o disco do sistema permanecerá inalterado. Para evitar a recriação desnecessária do disco, use a opção **Manter disco do sistema durante os ciclos de energia**, disponível na página **Configuração do Catálogo de Máquinas > Configurações de Disco**. Habilitar a opção reduz os tempos de reinicialização da VM, mas aumenta seus custos de armazenamento. A opção pode ser útil em

cenários onde um ambiente contém cargas de trabalho com tempos de reinicialização sensíveis. Para obter mais informações, consulte Otimização de armazenamento MCS.

- **O Studio agora oferece suporte à criação de catálogos de máquinas MCS com disco de cache de gravação persistente**. Anteriormente, o PowerShell era sua única opção para criar um catálogo com disco de cache de gravação persistente. Agora você pode usar o Studio para controlar se o disco de cache de gravação persiste para as VMs provisionadas no Azure ao criar um catálogo. Se desativado, o disco de cache de gravação é excluído durante cada ciclo de energia para economizar custos de armazenamento, fazendo com que quaisquer dados redirecionados para o disco sejam perdidos. Para reter os dados, habilite a opção **Usar disco de cache de gravação persistente**, disponível na página **Configuração do Catálogo de Máquinas > Configurações de Disco**. Para obter mais informações, consulte Otimização de armazenamento MCS.

Suporte para proteção de aplicativos para o serviço Citrix Virtual Apps and Desktops com StoreFront. Para obter mais informações, consulte a proteção de aplicativos.

Janeiro de 2021

Novos recursos disponíveis no Web Studio. Os seguintes recursos agora estão disponíveis no console baseado na web:

- **O Studio agora oferece suporte à associação de aplicativos com ícones personalizados**. Anteriormente, você tinha que usar o PowerShell para adicionar ícones personalizados para uso com aplicativos publicados. Agora você também pode usar o Studio para fazer isso. Para obter mais informações, consulte Gerenciar grupos de aplicativos.
- **O Studio agora oferece suporte à aplicação de tags a catálogos de máquinas**. Anteriormente, você poderia usar o Studio para criar ou excluir tags para uso com um catálogo. No entanto, você tinha que usar o PowerShell para aplicar tags ao catálogo. Agora você também pode usar o Studio para aplicar ou remover uma tag de um catálogo, assim como faz com grupos de entrega. Para obter mais informações, consulte Aplicar tags a catálogos de máquinas.
- **O Studio agora oferece suporte à alternância entre os modos de "balanceamento de carga horizontal" e "balanceamento de carga vertical"**. Anteriormente, o PowerShell era sua única opção para alternar entre os modos de balanceamento de carga horizontal e vertical. O Studio agora oferece mais flexibilidade para controlar como balancear a carga de máquinas de SO de sessão múltipla. Para obter mais informações, consulte Balancear carga de máquinas.

- **O Studio agora oferece suporte à inclusão de máquinas em modo de manutenção em agendamentos de reinicialização**. Anteriormente, o PowerShell era sua única opção para configurar reinicializações agendadas para máquinas em modo de manutenção. Agora você também pode usar o Studio para controlar se deseja incluir essas máquinas em um agendamento de reinicialização. Para obter mais informações, consulte Criar um agendamento de reinicialização.
- **O Studio agora oferece suporte à configuração de Wake on LAN para Acesso Remoto a PC**. Anteriormente, você tinha que usar o PowerShell para configurar o Wake on LAN para Acesso Remoto a PC. Agora você também pode usar o Studio para configurar o recurso. Para obter mais informações, consulte Configurar Wake on LAN.
- **O Studio agora oferece suporte à aplicação de propriedades de instância AWS e à marcação de recursos operacionais**. Ao criar um catálogo para provisionar máquinas na AWS usando o MCS, você pode especificar se deseja aplicar a função IAM e as propriedades de tag a essas máquinas. Você também pode especificar se deseja aplicar tags de máquina a recursos operacionais. Você tem as duas opções a seguir:
  - **Aplicar propriedades de modelo de máquina a máquinas virtuais**
  - **Aplicar tags de máquina a recursos operacionais**

  Para obter mais informações, consulte Aplicando propriedades de instância AWS e marcando recursos operacionais.
- **Host dedicado AWS**. O Citrix Studio agora adiciona uma opção chamada **Usar host dedicado** à página **Configuração do Catálogo de Máquinas > Segurança**. Essa configuração é adequada para implantações com restrições de licenciamento ou requisitos de segurança que exigem o uso de um host dedicado. Com um host dedicado, você possui um host físico inteiro e é cobrado por hora. Possuir esse host permite que você crie quantas instâncias EC2 o host permitir, sem custos adicionais. Para obter mais informações, consulte Tenancy AWS.
- **O Studio agora oferece suporte à execução imediata de um agendamento de reinicialização**. O Studio agora permite que você execute um agendamento de reinicialização imediatamente para reiniciar todas as máquinas aplicáveis no agendamento. Para obter mais informações, consulte Executar um agendamento de reinicialização imediatamente.
- **Autoscale**. O Autoscale oferece os seguintes novos recursos e aprimoramentos:
  - **O Studio agora oferece suporte à exibição de máquinas em estado de drenagem**. Anteriormente, o PowerShell era sua única opção para identificar máquinas em estado de drenagem. Agora você pode usar o Studio para identificar máquinas que estão em estado

de drenagem. Para obter mais informações, consulte Exibir máquinas em estado de drenagem.

- **O Studio agora oferece suporte à definição de horários de pico em um nível granular de 30 minutos para grupos de entrega VDI**. Anteriormente, você precisava usar o PowerShell para definir os horários de pico para os dias incluídos em um agendamento em um nível granular de 30 minutos para grupos de entrega VDI. Agora você também pode usar o Studio para fazer isso. Esse suporte permite que você defina o número mínimo de máquinas em execução em um Grupo de Entrega VDI separadamente para cada meia hora do dia.

Galeria de Imagens Compartilhadas do Azure. O serviço Citrix Virtual Apps and Desktops oferece suporte à Galeria de Imagens Compartilhadas do Azure como um repositório de imagens publicado para máquinas provisionadas por MCS no Azure. Os administradores têm a opção de armazenar uma imagem na galeria para acelerar a criação e a hidratação de discos de SO a partir da imagem mestre. Esse processo melhora os tempos de inicialização e de lançamento de aplicativos para VMs não persistentes.

A galeria contém os três elementos a seguir:

- Galeria. As imagens são armazenadas aqui. O MCS cria uma galeria para cada catálogo de máquinas.
- Definição de Imagem da Galeria. Essa definição inclui informações (tipo e estado do sistema operacional, região do Azure) sobre a imagem mestre. O MCS cria uma definição de imagem para cada imagem mestre criada para o catálogo.
- Versão da Imagem da Galeria. Cada imagem em uma Galeria de Imagens Compartilhadas pode ter várias versões, e cada versão pode ter várias réplicas em diferentes regiões. Cada réplica é uma cópia completa da imagem mestre. O serviço Citrix Virtual Apps and Desktops sempre cria uma versão de imagem Standard_LRS (versão 1.0.0) para cada imagem com o número apropriado de réplicas na região do catálogo. Essa configuração é baseada no número de máquinas no catálogo, na taxa de réplica configurada e no máximo de réplicas configurado.

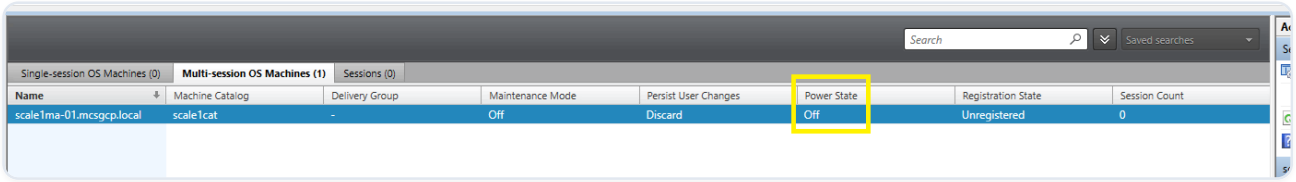
> **Nota:**
>
> A funcionalidade da Galeria de Imagens Compartilhadas funciona apenas com discos gerenciados. Não está disponível para catálogos de máquinas legados.

> Para obter detalhes sobre este recurso, consulte Configurar galeria de imagens compartilhadas.

Buckets de armazenamento criados na mesma região do Google Cloud Platform que o catálogo de máquinas. Em versões anteriores, o MCS criava buckets de armazenamento temporários durante o provisionamento como parte do processo de upload de disco. Esses buckets abrangiam várias regiões, que o Google define como uma grande área geográfica contendo dois ou mais locais geográficos. Esses buckets temporários residiam na localização geográfica dos Estados Unidos, independentemente de onde o catálogo fosse provisionado. O MCS agora cria buckets de armazenamento na mesma região onde você provisiona seus catálogos. Os buckets de armazenamento não são mais temporários; eles permanecem em seu projeto do Google Cloud Platform após a conclusão do processo de provisionamento. Futuras operações de provisionamento usarão o bucket de armazenamento existente. Se um existir nessa região, ou um novo bucket de armazenamento será criado se um não existir na região especificada.

Opção do PowerShell que define o padrão para reutilizar VDAs agrupados durante uma interrupção. Uma nova opção de comando do PowerShell (`-DefaultReuseMachinesWithoutShutdownInOutage`) estende a capacidade de reutilizar VDAs de desktop agrupados que não foram desligados durante uma interrupção, por padrão. Consulte Suporte a aplicativos e desktops.

Provisionamento sob demanda do Google Cloud Platform. O serviço Citrix Virtual Apps and Desktops atualiza a forma como o Google Cloud Platform (GCP) provisiona catálogos de máquinas. Ao criar um catálogo de máquinas, a instância de máquina correspondente não é criada no GCP e o estado de energia é definido como **OFF**. As máquinas não são provisionadas no momento da criação do catálogo, mas sim na primeira vez que as máquinas são ligadas. Por exemplo, depois de criar um catálogo, o estado de energia da VM é definido como **Off**:



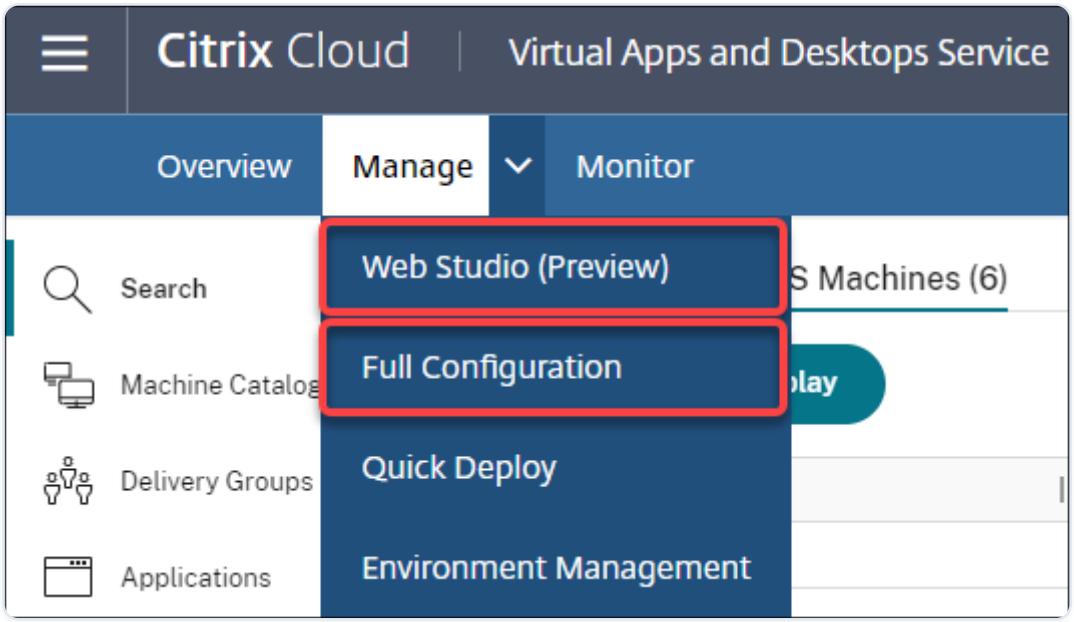
Dezembro de 2020

Recursos novos e aprimorados

O Web Studio está disponível como uma prévia. Um novo console baseado na web está agora disponível. Estamos em processo de migração de todo o conjunto de funcionalidades do Studio do

console legado para o novo console baseado na web. O console baseado na web geralmente responde mais rápido que o console legado. Por padrão, você faz login automaticamente no console baseado na web. Você pode alternar facilmente entre o console baseado na web e o console legado na guia **Gerenciar** para realizar suas tarefas de configuração ou gerenciamento de site. Clique na seta para baixo ao lado de **Gerenciar** e selecione uma opção:

- **Web Studio (Prévia)**. Leva você ao novo console baseado na web.
- **Configuração Completa**. Leva você ao console legado.



Os seguintes recursos estão disponíveis apenas no console baseado na web:

- **Suporte para tipo de disco SSD padrão para Azure**. O Studio agora adiciona suporte para o tipo de disco SSD padrão. Os SSDs padrão do Azure são uma opção de armazenamento econômica otimizada para cargas de trabalho que precisam de desempenho consistente em níveis de IOPS mais baixos. Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem mestre do Azure Resource Manager.
- **O Studio agora oferece suporte à configuração do atraso de desligamento para grupos de entrega VDI estáticos**. Anteriormente, você só podia configurar o atraso de desligamento para grupos de entrega VDI estáticos por meio do SDK do PowerShell. O Studio agora permite configurar o atraso de desligamento na interface do usuário do Autoscale para grupos de entrega VDI estáticos. Para obter mais informações, consulte Autoscale.

Outubro de 2020

Recursos novos e aprimorados

Descartar vários alertas de hipervisor. O Citrix Monitor agora oferece suporte ao descarte automático de alertas de hipervisor com mais de um dia. Para obter mais informações, consulte Monitoramento de Alertas de Hipervisor.

Remover endereço IP externo. Um endereço IP externo em uma máquina virtual temporária que é usada para preparar uma imagem provisionada no Google Cloud Platform (GCP) não é mais necessário. Este endereço IP externo permite que a máquina virtual temporária acesse a API pública do Google para concluir o processo de provisionamento.

Habilite o Acesso Privado do Google para permitir que a VM acesse a API pública do Google diretamente da sub-rede. Para obter mais informações, consulte Habilitar acesso privado do Google.

Novo modelo aborda como as identidades de máquina são gerenciadas. As identidades de máquina usadas em catálogos de máquinas foram gerenciadas e mantidas usando o Active Directory. Todas as máquinas criadas pelo MCS agora serão unidas ao Active Directory. O novo modelo de serviço Citrix Virtual Apps and Desktops aborda como as identidades de máquina são gerenciadas. Este modelo permite a criação de catálogos de máquinas usando *grupo de trabalho*, ou máquinas não unidas ao domínio.

> **Dica:**
>
> Essa funcionalidade oferece suporte a um novo serviço de identidade, *confiança FMA*, adicionado ao Citrix Cloud para máquinas não unidas ao domínio.
>
> O MCS se comunica com o novo serviço de confiança FMA para gerenciamento de identidade. As informações de identidade são armazenadas no disco de identidade como um par de GUID e pares de chaves privadas, em vez do paradigma de SID de domínio e senha de conta de máquina usado pelo Active Directory. Os VDAs que usam máquinas não unidas ao domínio usam essa combinação de GUID e chave privada para registro do broker. Para obter mais informações, consulte Configurar suporte para catálogos não unidos ao domínio.

Usar upload direto para discos gerenciados do Azure. Esta versão permite que você use o upload direto ao criar discos gerenciados em um ambiente Azure. Essa funcionalidade reduz os custos associados a contas de armazenamento extras. Você não precisa mais preparar o VHD em

uma conta de armazenamento antes de convertê-lo em um disco gerenciado. Além disso, o upload direto elimina a necessidade de anexar um disco gerenciado vazio a uma máquina virtual. O upload direto para um disco gerenciado do Azure simplifica o fluxo de trabalho, permitindo que você copie um VHD local diretamente para uso como um disco gerenciado. Os discos gerenciados suportados incluem Standard HDD, Standard SSD e Premium SSD.

Para obter mais informações sobre este recurso, consulte o blog do Microsoft Azure.

Para obter mais informações sobre discos gerenciados do Azure, consulte a página de documentação.

Grupo de Recursos Único no Azure. Agora você pode criar e usar um único grupo de recursos do Azure para atualizar e criar catálogos no Citrix Virtual Apps and Desktops. Este aprimoramento se aplica a entidades de serviço de escopo total e de escopo restrito. O limite anterior de 240 VMs por 800 discos gerenciados por Grupo de Recursos do Azure foi removido. Não há mais limite para o número de máquinas virtuais, discos gerenciados, snapshots e imagens por Grupo de Recursos do Azure.

Para obter mais informações, consulte Ambientes de virtualização do Microsoft Azure Resource Manager.

Setembro de 2020

Novos recursos e aprimoramentos

Implantação Rápida. O novo recurso Implantação Rápida substitui o antigo Azure Quick Deploy. O novo recurso oferece uma maneira rápida de começar a usar o serviço Citrix Virtual Apps and Desktops com o Microsoft Azure. Você pode usar a Implantação Rápida para entregar desktops e aplicativos e configurar o Acesso Remoto ao PC.

Administrador de Sessão (função interna). O Citrix Studio agora adiciona uma nova função interna chamada **Administrador de Sessão**. A função permite que um administrador visualize grupos de entrega e gerencie suas sessões e máquinas associadas na página **Filtros** da guia **Monitor**. Com esse recurso, você pode configurar as permissões de acesso de administradores existentes ou administradores que você convida de uma forma que se alinhe com sua função em sua organização. Para obter mais informações sobre a função interna, consulte Funções e escopos internos. Para obter informações sobre como atribuir a função interna a um administrador, consulte Administração e monitoramento delegados.

Para um nível mais granular de controle sobre o acesso à página **Filtros** relacionada a sessões e máquinas, crie uma função personalizada e selecione uma das seguintes opções para o objeto Director: **Exibir página de Filtros - Somente máquinas**, **Exibir página de Filtros - Somente sessões**. Para obter informações sobre como criar uma função personalizada, consulte Criar e gerenciar funções.

Suporte para um novo tipo de máquina. Esta versão adiciona suporte para as séries NV v4 e DA v4 de máquinas AMD, ao configurar Discos Premium para um catálogo de máquinas. Para obter mais informações, consulte Criar grupos de entrega.

Agosto de 2020

Novos recursos e aprimoramentos

Acesso limitado ao SDK do PowerShell Remoto durante uma interrupção. Anteriormente, você não podia usar comandos do PowerShell durante uma interrupção. Agora, o Cache de Host Local permite acesso limitado ao SDK do PowerShell Remoto durante uma interrupção. Consulte O que está indisponível durante uma interrupção.

Suporte para duas novas edições do serviço Citrix Virtual Apps and Desktops. O Citrix Monitor agora oferece suporte a duas novas edições do serviço Citrix Virtual Apps and Desktops, a saber, **Citrix Virtual Apps Advanced service** e **Citrix Virtual Apps and Desktops Advanced service**. Para obter mais informações, consulte a Matriz de compatibilidade de recursos do Citrix Monitor.

Suporte para Virtual Private Cloud (VPC) compartilhada no Google Cloud Platform. O serviço Citrix Virtual Apps and Desktops oferece suporte a VPC Compartilhada no Google Cloud Platform como um recurso de host. Você pode usar o Machine Creation Services (MCS) para provisionar máquinas em uma VPC Compartilhada e gerenciá-las usando o Citrix Studio. Para obter informações sobre VPC Compartilhada, consulte Virtual Private Cloud Compartilhada.

Suporte à seleção de zona para Google Cloud Platform. O serviço Citrix Virtual Apps and Desktops oferece suporte à seleção de zona no Google Cloud Platform. Esse recurso permite que os administradores especifiquem uma ou várias zonas dentro de uma região para a criação de catálogos.

Para VMs do tipo de locatário único, a seleção de zona oferece aos administradores a capacidade de colocar nós de locatário único em zonas de sua escolha. Para VMs que não são de locatário único, a seleção de zona oferece a capacidade de colocar VMs de forma determinística em zonas

de sua escolha, proporcionando assim flexibilidade no design da implantação. Para obter informações de configuração, consulte Habilitar seleção de zona.

Além disso:

- A locação única oferece acesso exclusivo a um nó de locatário único, que é um servidor físico de mecanismo de computação dedicado a hospedar apenas as VMs do seu projeto. Esses nós permitem agrupar suas VMs no mesmo hardware ou separar suas VMs das VMs de outros projetos.
- Os nós de locatário único ajudam você a atender aos requisitos de hardware dedicado para cenários de Bring Your Own License (BYOL). Eles também permitem que você cumpra a política de controle de acesso à rede, segurança e requisitos de privacidade, como HIPAA.

> **Nota:**
>
> A locação exclusiva é a única maneira de usar implantações de VDI do Windows 10 no Google Cloud. O VDI de servidor também oferece suporte a esse método. Uma descrição detalhada para locação exclusiva pode ser encontrada no site de documentação do Google.

> **Desempenho de inicialização aprimorado para discos de sistema do Azure**. Esta versão oferece suporte a um desempenho de inicialização aprimorado para implementações do Citrix Cloud usando o Azure quando o MCSIO está habilitado. Com esse suporte, você pode reter o disco do sistema. Isso oferece as seguintes vantagens:

- As VMs e os aplicativos agora inicializam e são iniciados com desempenho semelhante à forma como a imagem dourada é servida.
- Redução no consumo de cota da API, na exclusão e criação do disco do sistema e no atraso de transição de estado causado ao excluir uma VM.

Por exemplo, use a propriedade personalizada `PersistOSDisk` do PowerShell no comando `New-ProvScheme` para configurar esse recurso.

```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>'
```

Para obter mais informações de configuração, consulte Melhorar o desempenho de inicialização.

Julho de 2020

Recursos novos e aprimorados

Suporte para acesso granular baseado em função à página Filtros. O Citrix Studio agora oferece controle mais granular sobre o acesso à página **Monitor > Filtros** ao criar uma função personalizada. Especificamente, você pode atribuir permissões para visualizar qualquer combinação de **Máquinas**, **Sessões**, **Conexões** e **Instâncias de Aplicativo** a uma função personalizada. A seguir estão mais quatro opções para o objeto **Director** na janela **Criar Função**:

- Exibir página Filtros - Somente Instâncias de Aplicativo
- Exibir página Filtros - Somente Conexões
- Exibir página Filtros - Somente Máquinas
- Exibir página Filtros - Somente Sessões

Para obter informações sobre como criar funções, consulte Criar e gerenciar funções.

Suporte para atraso de desligamento para máquinas VDI atribuídas (somente PowerShell). Em versões anteriores, o atraso de desligamento aplicava-se apenas a máquinas não atribuídas. A partir desta versão, o atraso de desligamento aplica-se a máquinas atribuídas e não atribuídas. Para obter mais informações, consulte Como o Autoscale gerencia a energia das máquinas.

Suporte para licenças de Cliente Windows. O serviço Citrix Virtual Apps and Desktops agora oferece suporte ao uso de licenças de Cliente Windows para provisionar VMs no Azure. Para executar VMs do Windows 10 no Azure, verifique se seu contrato de licenciamento por volume com a Microsoft se qualifica para este uso. Para obter mais informações, consulte Criar um catálogo de máquinas usando uma imagem mestre do Azure Resource Manager.

Maio de 2020

Recursos novos e aprimorados

Agendamentos de reinicialização de máquinas. Agora você pode indicar se um agendamento de reinicialização afeta máquinas que estão em modo de manutenção. Este recurso está disponível apenas no PowerShell. Para obter detalhes, consulte Reinicializações agendadas para máquinas em modo de manutenção.

Disponibilidade de recursos. Agora você pode garantir a disponibilidade de recursos durante uma interrupção sem precisar publicar recursos em todas as zonas (localização de recursos). Para obter detalhes, consulte Disponibilidade de recursos.

Abril de 2020

Recursos novos e aprimorados

Granularidade de agendamento aprimorada para Grupos de Entrega VDI (somente PowerShell). O Autoscale agora oferece suporte à definição dos horários de pico para os dias incluídos em um agendamento em um nível granular de 30 minutos. Você pode definir o número mínimo de máquinas em execução em um Grupo de Entrega VDI separadamente para cada meia hora do dia. Além disso, o Autoscale agora pode aumentar ou diminuir o número de máquinas ligadas em Grupos de Entrega VDI a cada meia hora, em vez de a cada hora. Para obter mais informações, consulte Comandos do SDK do Broker PowerShell.

Descoberta de MTU. O protocolo Citrix Enlightened Data Transport (EDT) agora possui recursos de Descoberta de MTU. A Descoberta de MTU permite que o EDT determine e defina automaticamente o tamanho da carga útil para a sessão. Este recurso permite que a sessão ICA se ajuste a redes com requisitos não padrão de Unidade Máxima de Transmissão (MTU) ou Tamanho Máximo de Segmento (MSS). A capacidade de ajuste evita a fragmentação de pacotes que pode resultar em desempenho degradado ou falha no estabelecimento de uma sessão ICA. Esta atualização requer no mínimo o Citrix Workspace app 1911 para Windows. Se estiver usando o Citrix Gateway, a versão mínima de firmware do Citrix ADC necessária é 13.0.52.24 ou 12.1.56.22. Para obter mais informações, consulte Descoberta de MTU do EDT.

Março de 2020

Recursos novos e aprimorados

Métricas de dispositivo de destino PVS. O Citrix Monitor agora fornece um painel de métricas de dispositivo de destino PVS na página Detalhes da Máquina. Use o painel para visualizar o

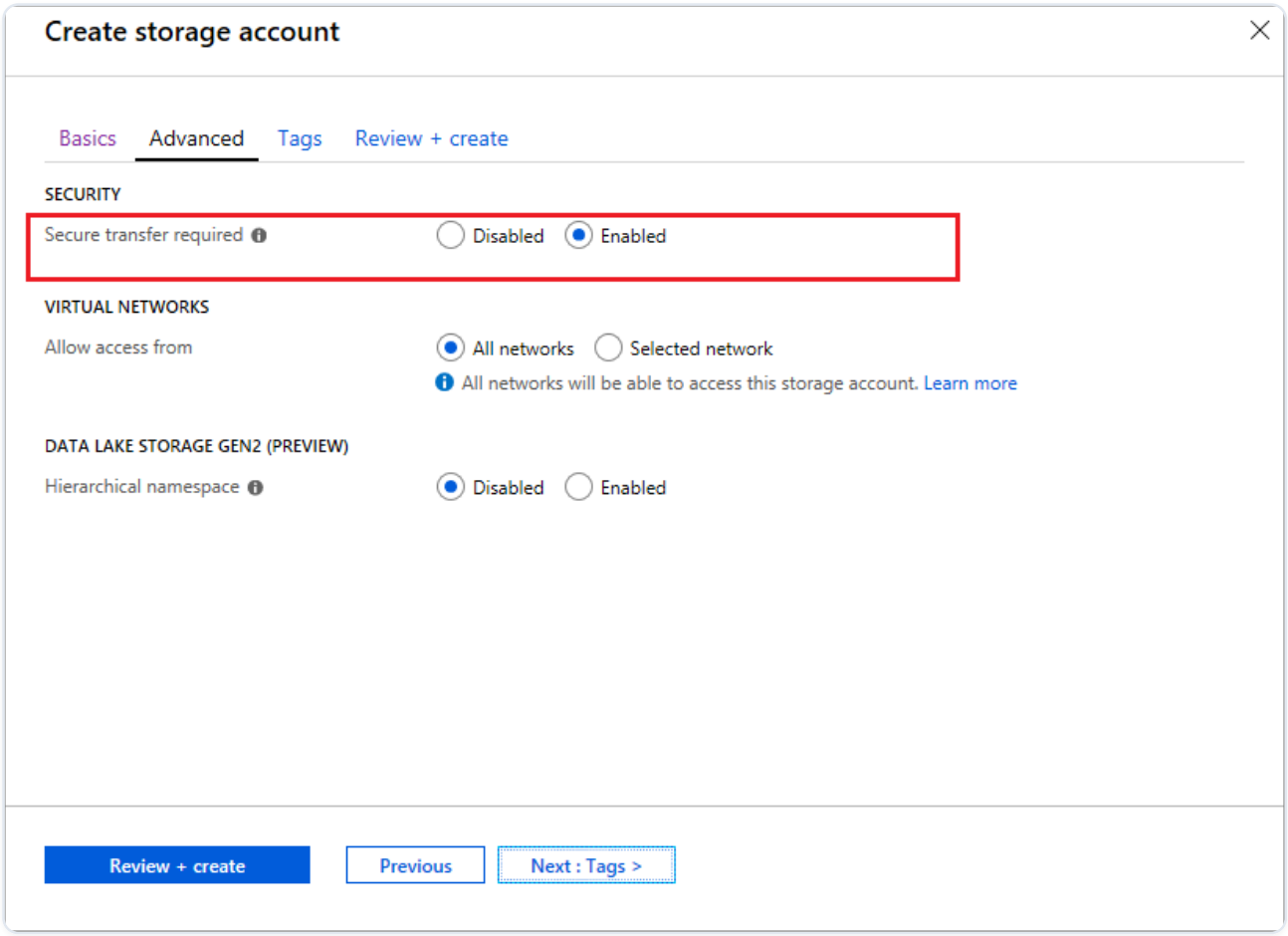
status dos dispositivos de destino de Provisionamento para máquinas de SO de sessão única e multi-sessão. Várias métricas para Rede, Inicialização e Cache estão disponíveis neste painel. Essas métricas ajudam você a monitorar e solucionar problemas de dispositivos de destino PVS para garantir que estejam funcionando. Para obter mais informações, consulte Métricas de dispositivo de destino PVS.

Captura de propriedades de instância AWS. O MCS agora lê as propriedades da instância da qual a AMI foi tirada e aplica a função IAM e as tags da máquina às máquinas provisionadas para um determinado catálogo. Ao usar este recurso opcional, o processo de criação do catálogo encontra a instância de origem da AMI selecionada, lendo um conjunto limitado de propriedades. Essas propriedades são então armazenadas em um Modelo de Inicialização da AWS, que é usado para provisionar máquinas para esse catálogo. Qualquer máquina no catálogo herda as propriedades da instância capturadas. Para obter mais informações, consulte Captura de propriedades de instância AWS.

Marcação de recursos operacionais da AWS. Esta versão introduz uma opção para marcar recursos criados por componentes Citrix durante o provisionamento. Cada tag representa um rótulo que consiste em uma chave definida pelo cliente e um valor opcional que melhora sua capacidade de gerenciar, pesquisar e filtrar recursos. Para obter mais informações, consulte Marcação de recursos operacionais da AWS.

Transferência segura no armazenamento do Azure. O Machine Creation Services (MCS) oferece um aprimoramento para contas de armazenamento criadas por catálogos provisionados por MCS em ambientes do Azure Resource Manager. Este aprimoramento habilita automaticamente a propriedade de transferência segura necessária. Esta opção aumenta a segurança da conta de armazenamento, permitindo apenas solicitações para a conta a partir de conexões seguras. Para obter mais informações, consulte Exigir transferência segura para garantir conexões seguras no site da Microsoft.

Habilite a propriedade **Transferência segura necessária** ao criar uma conta de armazenamento no Azure:



Suporte para discos gerenciados SSD do Azure. O Machine Creation Services (MCS) oferece suporte a discos gerenciados SSD padrão para máquinas virtuais do Azure. Este tipo de disco oferece desempenho consistente e maior disponibilidade em comparação com discos HDD. Para obter mais informações, consulte Discos SSD padrão para cargas de trabalho de máquinas virtuais do Azure.

Use a propriedade personalizada `StorageAccountType` do PowerShell no comando `New-ProvScheme` ou no comando `Set-ProvScheme` para configurar este recurso:

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /><Property
xsi:type=`"StringProperty`" Value=`"Windows_Server`" />
```

Nota:

Este recurso está disponível apenas ao usar discos gerenciados, ou seja, a propriedade personalizada `UseManagedDisks` está definida como **true**. Para discos não gerenciados, apenas HDD padrão e SSD Premium são suportados.

Janeiro de 2020

Recursos novos e aprimorados

Barra de idiomas no Citrix Studio. A partir desta versão, o Citrix Studio oferece uma barra de idiomas para facilitar o mapeamento correto do teclado.

- Se o idioma do Citrix Cloud ou o idioma de exibição do seu navegador estiver definido como **Inglês** ou **Japonês**, a barra de idiomas não aparece.
- Se o idioma do Citrix Cloud ou o idioma de exibição do seu navegador estiver definido como **Alemão**, **Espanhol** ou **Francês**, a barra de idiomas aparece depois que você faz logon no Citrix Studio. Existem duas opções de idioma na lista da barra de idiomas. Selecione uma opção que corresponda ao idioma principal do seu navegador.

  > **Dica:**
  >
  > - As configurações que você configura para a barra de idiomas podem não ter efeito. Nesse caso, faça logoff e faça logon novamente.
  > - Você pode não conseguir inserir certos símbolos e caracteres localizados usando a barra de idiomas. Para resolver o problema, você precisa configurar o idioma do Citrix Cloud, o idioma de exibição do seu navegador e o layout do teclado local. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX310743.

Temporizador de atraso máximo do agendamento de reinício (somente PowerShell). Se um reinício agendado de máquinas em um Grupo de Entrega não iniciar devido a uma interrupção do banco de dados do site, você pode especificar quanto tempo esperar além do horário de início agendado. Se a conexão do banco de dados for restaurada durante esse intervalo, os reinícios começarão. Se a conexão não for restaurada durante esse intervalo, os reinícios não começarão. Para obter detalhes, consulte Reinícios agendados atrasados devido a interrupção do banco de dados.

Balanceamento de carga vertical (somente PowerShell). Anteriormente, o serviço usava balanceamento de carga horizontal para todos os lançamentos de RDS, que atribui a carga de entrada à máquina RDS menos carregada. Isso permanece o padrão. Agora, você pode usar o

PowerShell para habilitar o balanceamento de carga vertical como uma configuração em todo o site.

Quando o balanceamento de carga vertical está habilitado, o broker atribui a carga de entrada à máquina mais carregada que não atingiu uma marca d'água alta. Isso satura as máquinas existentes antes de passar para novas máquinas. À medida que os usuários se desconectam e liberam máquinas existentes, uma nova carga é atribuída a essas máquinas.

Por padrão, o balanceamento de carga horizontal está habilitado. Para visualizar, habilitar ou desabilitar o balanceamento de carga vertical, os cmdlets `Get-BrokerSite` e `Set-BrokerSite` agora suportam a configuração `UseVerticalScalingForRdsLaunches`. Para obter mais informações, consulte Gerenciar carga de máquinas em Grupos de Entrega.

Dezembro de 2019

Recursos novos e aprimorados

Serviço para Provedores de Serviços Citrix (CSP). Os CSPs agora podem integrar clientes locatários ao serviço Virtual Apps and Desktops, configurar o acesso de administrador do cliente ao serviço e fornecer espaços de trabalho compartilhados ou dedicados aos usuários dos clientes usando domínios federados. Para obter mais informações, consulte Serviço Citrix Virtual Apps and Desktops para Provedores de Serviços Citrix.

Suporte para determinar por que uma máquina está no modo de manutenção (somente PowerShell). Usando o PowerShell, agora você pode determinar por que uma máquina está no modo de manutenção. Para fazer isso, use o parâmetro `-MaintenanceModeReason`. O recurso é útil para administradores solucionarem problemas com máquinas no modo de manutenção. Para obter detalhes, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/Broker/Get-BrokerMachine/>`.

Autoscale. O Autoscale agora oferece a capacidade de criar e excluir máquinas dinamicamente. Você pode usar essa capacidade por meio de um script PowerShell. O script ajuda a escalar dinamicamente o número de máquinas no Grupo de Entrega para cima ou para baixo com base nas condições de carga atuais. Para obter mais informações, consulte Provisionar máquinas dinamicamente com Autoscale.

Novembro de 2019

Recursos novos e aprimorados

GroomStartHour. O Monitor agora suporta **GroomStartHour** - uma nova configuração que ajuda os administradores a determinar a hora do dia em que a limpeza deve começar a ser executada. Para obter mais informações, consulte a documentação do SDK do Citrix Virtual Apps and Desktops.

Paginação OData. O Monitor agora suporta **paginação OData**. Todos os endpoints OData v4 retornam um máximo de 100 registros por página com um link para os próximos 100 registros na resposta. Para obter mais informações, consulte Acessando dados do Serviço Monitor usando o endpoint OData v4 no Citrix Cloud.

Outubro de 2019

Recursos novos e aprimorados

App-V. A funcionalidade App-V agora está disponível no Citrix Cloud. Você pode adicionar pacotes App-V ao Delivery Controller em sua configuração do Citrix Cloud, no modo de administrador único ou duplo. O *módulo de descoberta de pacotes App-V do serviço Virtual Apps and Desktops*, disponível em Citrix Downloads, permite importar pacotes App-V e registrar servidores Microsoft App-V. Os aplicativos que eles contêm ficam então disponíveis para seus usuários. Este módulo PowerShell permite registrar servidores de Gerenciamento e Publicação do Microsoft App-V usando URLs DNS, evitando a necessidade de que os servidores por trás de mecanismos de balanceamento de carga sejam registrados usando sua URL de máquina real. Para obter mais informações, consulte Módulo de descoberta de serviço do Citrix Virtual Apps and Desktops para pacotes e servidores App-V.

Google Cloud Platform. O serviço Citrix Virtual Apps and Desktops agora adiciona suporte para usar o Machine Creation Services (MCS) para provisionar máquinas no Google Cloud Platform (GCP). Para obter mais informações, consulte Ambientes de virtualização do Google Cloud Platform.

Setembro de 2019

Recursos novos e aprimorados

Suporte a VDA para Azure Virtual Desktop. Para sistemas operacionais e versões de VDA compatíveis, consulte VDAs em um ambiente do Azure Virtual Desktop.

Política de energia aprimorada. Em versões anteriores, uma máquina VDI em transição para um período de tempo em que uma ação (ação de desconexão="**Suspender**" ou "**Desligar**") era necessária permanecia ligada. Esse cenário ocorria se a máquina fosse desconectada durante um período de tempo (horários de pico ou fora de pico) em que nenhuma ação (ação de desconexão="**Nada**") era necessária.

A partir desta versão, o Autoscale suspende ou desliga a máquina quando o tempo de desconexão especificado expira, dependendo da ação de desconexão configurada para o período de tempo de destino. Para obter mais informações, consulte Gerenciar energia de máquinas VDI em transição para um período de tempo diferente com sessões desconectadas.

Catálogos de máquinas: Tags. Agora você pode usar o PowerShell para aplicar tags a catálogos de máquinas. Para obter mais informações, consulte Aplicar tags a catálogos de máquinas.

Duração da inicialização da sessão. O Monitor agora exibe a duração da inicialização da sessão dividida em períodos de tempo de inicialização do Workspace App e do VDA. Esses dados ajudam você a entender e solucionar problemas de tempos elevados de inicialização da sessão. Além disso, a duração de cada fase envolvida no início da sessão ajuda na solução de problemas associados a fases individuais. Por exemplo, se o tempo de Mapeamento de Unidade for alto, você pode verificar se todas as unidades válidas estão mapeadas corretamente no GPO ou script. Este recurso está disponível em VDAs 1903 ou posteriores. Para obter mais informações, consulte Diagnosticar problemas de inicialização da sessão.

Agosto de 2019

Recursos novos e aprimorados

Reconexão Automática de Sessão. A página Sessões na guia Tendências agora inclui informações sobre o número de reconexões automáticas. As reconexões automáticas são tentadas quando as políticas de Confiabilidade da Sessão ou Reconexão Automática do Cliente estão em vigor. As informações de reconexão automática ajudam você a visualizar e solucionar problemas de conexões de rede com interrupções e também a analisar redes com uma experiência perfeita.

A análise detalhada fornece informações adicionais como Confiabilidade da Sessão ou Reconexão Automática do Cliente, carimbos de data/hora, IP do Endpoint e Nome do Endpoint da máquina onde o aplicativo Workspace está instalado. Este recurso está disponível para Citrix Workspace app para Windows, Citrix Workspace app para Mac, Citrix Receiver™ para Windows e Citrix Receiver para Mac. Este recurso requer VDAs 1906 ou posteriores. Para obter mais informações, consulte:

- Sessões
- Configurações da política de reconexão automática do cliente
- Configurações da política de confiabilidade da sessão
- Reconexão Automática de Sessão

Julho de 2019

Recursos novos e aprimorados

Registro de Configuração. Agora você pode usar o SDK do PowerShell Remoto para excluir periodicamente o conteúdo do banco de dados de Registro de Configuração. Para obter detalhes, consulte Agendar exclusão periódica de dados.

Autoscale. O Autoscale agora oferece a flexibilidade de gerenciar o consumo de energia de apenas um subconjunto de máquinas em um Grupo de Entrega. Esse recurso pode ser útil em casos de uso de cloud bursting, onde você deseja usar recursos locais para manipular cargas de trabalho antes que os recursos baseados em nuvem atendam a outras demandas (ou seja, cargas de trabalho de burst). Para obter mais informações, consulte Restringir o Autoscale a determinadas máquinas em um Grupo de Entrega.

Acesso a Aplicativos Locais e redirecionamento de URL. O Citrix Studio agora permite adicionar a opção Adicionar Aplicativo de Acesso a Aplicativos Locais à interface do usuário do Studio para o seu Site usando o SDK do PowerShell. Para obter mais informações, consulte Fornecer acesso apenas a aplicativos publicados.

Alterações nos nomes dos sistemas operacionais. Os nomes dos sistemas operacionais nas páginas **Criar Catálogo de Máquinas > Configuração do Catálogo de Máquinas > Sistema Operacional** e **Monitor** foram alterados:

- SO multissessão (anteriormente SO de Servidor): O catálogo de máquinas de SO multissessão fornece desktops compartilhados hospedados para uma implantação em larga escala de máquinas Windows multissessão ou Linux padronizadas.
- SO de sessão única (anteriormente SO de Desktop): O catálogo de máquinas de SO de sessão única fornece desktops VDI ideais para vários usuários.

Duração do Citrix Profile Management no Carregamento de Perfil. O Monitor agora inclui a duração do processamento do perfil na barra Carregamento de Perfil do gráfico de duração de Logon. Esta é a duração que o Citrix Profile Management leva para processar perfis de usuário. Essas informações ajudam os administradores a solucionar problemas de durações de

carregamento de perfil altas com maior precisão. Este aprimoramento está disponível em VDAs 1903 e posteriores. Para obter mais informações, consulte Carregamento de Perfil.

Sondagem de desktop. A sondagem de desktop é um recurso do serviço Citrix Virtual Apps and Desktops. Ela automatiza as verificações de integridade de desktops virtuais publicados em um site, o que melhora a experiência do usuário. Para iniciar a sondagem de desktop, instale e configure o Citrix Probe Agent em um ou mais endpoints. A sondagem de desktop está disponível para Sites com licença Premium. Este recurso requer o Citrix Probe Agent 1903 ou posterior. Para obter mais informações, consulte Sondagem de Aplicativos e Desktops.

> **Nota:**
>
> O Citrix Probe Agent agora oferece suporte a TLS 1.2.

Junho de 2019

Recursos novos e aprimorados

Restringir por tags. Tags são strings que identificam itens como máquinas, aplicativos, desktops, Grupos de Aplicativos e políticas. Depois de criar uma tag e adicioná-la a um item, você pode adaptar certas operações para que se apliquem apenas a itens que tenham uma tag especificada. Para obter mais informações, consulte Grupos de Aplicativos e Tags.

Notificações por e-mail. O serviço Citrix Virtual Apps and Desktops envia notificações por e-mail relacionadas a alertas e sondagens diretamente. Isso elimina a necessidade de configurar o servidor de e-mail SMTP. A caixa **Preferências de Notificação** é habilitada por padrão e o Citrix Cloud envia notificações de alerta para os endereços de e-mail fornecidos na seção **Preferências de Notificação**. Certifique-se de que o endereço de e-mail `donotreplynotifications@citrix.com` esteja na lista de permissões em sua configuração de e-mail.

Maio de 2019

Recursos novos e aprimorados

Autoscale. O Autoscale é um recurso do serviço Citrix Virtual Apps and Desktops que fornece uma solução consistente e de alto desempenho para gerenciar proativamente a energia de suas máquinas. Ele visa equilibrar custos e experiência do usuário. O Autoscale incorpora a tecnologia Smart Scale, que foi descontinuada, na solução de gerenciamento de energia do Studio. Para

obter mais informações, consulte Autoscale. Você pode monitorar as métricas de máquinas gerenciadas pelo Autoscale nas páginas de Tendências no console **Monitor**. Para obter mais informações, consulte Monitorar máquinas gerenciadas pelo Autoscale.

Fevereiro de 2019

Recursos novos e aprimorados

Monitoramento de alertas do hipervisor. Os alertas do Citrix Hypervisor e do VMware vSphere agora são exibidos na guia **Monitor** > **Alertas** para ajudar a monitorar os seguintes estados/parâmetros de integridade do hipervisor:

- Uso da CPU
- Uso da memória
- Uso da rede
- Conexão do hipervisor indisponível
- Uso do disco (somente vSphere)
- Conexão do host ou estado de energia (somente vSphere)

Para obter mais informações, consulte a seção Monitoramento de alertas do hipervisor em Alertas e Notificações.

Comunicações sobre versões anteriores do TLS. Para melhorar a segurança do serviço, a Citrix bloqueará qualquer comunicação sobre Transport Layer Security (TLS) 1.0 e 1.1 a partir de March 15, 2019, permitindo apenas comunicações TLS 1.2. Para obter mais informações, consulte Versões do TLS. Para obter orientações abrangentes, consulte CTX247067.

Grupos de Aplicativos. Os Grupos de Aplicativos permitem gerenciar coleções de aplicativos. Você pode criar Grupos de Aplicativos para aplicativos compartilhados entre diferentes Grupos de Entrega ou usados por um subconjunto de usuários dentro dos Grupos de Entrega. Para obter mais informações, consulte Criar Grupos de Aplicativos.

Desempenho de Logon - Detalhamento de Perfil. O painel **Duração do Logon** na página **Detalhes do Usuário** em **Monitor** agora inclui informações sobre o detalhamento da **fase de carregamento do perfil** do processo de logon. O detalhamento do perfil fornece informações úteis sobre os perfis de usuário para a sessão atual que podem ajudar os administradores a solucionar problemas de alto carregamento de perfil. Uma dica de ferramenta com as seguintes informações de perfis de usuário é exibida:

- Número de arquivos

- Tamanho do perfil
- Número de arquivos grandes

Um detalhamento fornece informações sobre as pastas individuais, seu tamanho e o número de arquivos. Este recurso está disponível em VDAs 1811 e posteriores. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Integridade da licença Microsoft RDS. Monitore o status da licença Microsoft RDS (Remote Desktop Services) no painel **Detalhes da Máquina** nas páginas Detalhes da Máquina e Detalhes do Usuário para máquinas com SO de Servidor. Uma mensagem apropriada é exibida para o status da licença. Você pode passar o mouse sobre o ícone de informações para ver mais detalhes. Para obter mais informações, consulte a seção Integridade da licença Microsoft RDS em Solução de problemas de máquinas.

Sondagem de Aplicativos. Este recurso automatiza a avaliação da integridade dos Aplicativos Virtuais publicados em um Site.

Para iniciar a sondagem de aplicativos:

- Em uma ou mais máquinas de endpoint, instale o Citrix Application Probe Agent
- Configure o Citrix Application Probe Agent com as credenciais do Citrix Workspace e do serviço Citrix Virtual Apps and Desktops.
- Configure os aplicativos a serem sondados, as máquinas de endpoint para executar a sondagem e o tempo de sondagem agendado em **Monitor** > **Configuração** do serviço Citrix Virtual Apps and Desktops.

O agente testa o lançamento dos aplicativos selecionados via Citrix Workspace e reporta os resultados da sondagem no console **Monitor** do serviço Citrix Virtual Apps and Desktops em:

- a página Aplicativos – os dados das últimas 24 horas e a página **Tendências** > **Resultados da Sondagem de Aplicativos**
- os dados históricos da sondagem, juntamente com o estágio em que a falha da sondagem ocorreu - Acessibilidade do Workspace, Autenticação do Workspace, Enumeração do Workspace, download do ICA ou inicialização do Aplicativo

O relatório de falha é enviado por e-mail para os endereços de e-mail configurados. Você pode agendar sondagens de aplicativos para serem executadas durante o horário de pico em vários locais geográficos. Dessa forma, você pode usar os resultados para solucionar proativamente problemas relacionados a aplicativos provisionados, máquinas de hospedagem ou conexões

antes que os usuários os experimentem. Para obter mais informações, consulte Sondagem de Aplicativos e Desktops.

Janeiro de 2019

Recursos novos e aprimorados

Administração Delegada com escopo personalizado. O monitoramento agora oferece suporte a escopo personalizado para funções de administrador delegado integradas. Para obter mais informações sobre as funções integradas disponíveis para monitoramento e como atribuí-las, consulte Funções de administrador delegado.

Dezembro de 2018

Recursos novos e aprimorados

A data após a qual a Citrix bloqueará a comunicação por meio do Transport Layer Security (TLS) 1.0 e 1.1 foi alterada de December 31, 2018 para January 31, 2019. Para obter detalhes, consulte Descontinuação das versões TLS.

Novembro de 2018

Recursos novos e aprimorados

Dados históricos da máquina disponíveis usando a API OData: Dados históricos contendo análises da máquina agora estão disponíveis por meio da API OData. Esses dados são coletados a cada hora e acumulados para o dia.

- Número de máquinas ligadas (para máquinas com gerenciamento de energia)
- Número de máquinas registradas
- Número de máquinas em modo de manutenção
- Número total de máquinas

Os dados são agregados para o período durante o qual o Serviço de Monitoramento está em execução. Para obter mais informações sobre o uso da API OData e exemplos, consulte Citrix Monitor Service 7 1808. O esquema do banco de dados está disponível em Monitor Service Schema.

Desempenho de Logon - Detalhamento da sessão interativa: O painel **Duração do Logon** na exibição **Detalhes do Usuário e da Sessão** inclui informações sobre a fase **Sessão Interativa** do processo de logon. O tempo gasto em cada uma das três subfases (**Pre-userinit**, **Userinit** e

Shell) é exibido na barra **Sessão Interativa** como uma dica de ferramenta. Isso fornece uma solução de problemas e remediação mais granulares para esta fase do logon. O atraso de tempo cumulativo entre as subfases e um link para a documentação também são fornecidos. Este recurso está disponível no Delivery Controller versão 7 1808 e posterior. A barra de detalhamento da **Sessão Interativa** mostra a duração do tempo apenas para a sessão atual. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Desempenho de Logon - Detalhamento de GPO: O painel **Duração do Logon** na exibição de detalhes de **Usuário e Sessão** contém a duração do GPO (Objetos de Política de Grupo). Este é o tempo total gasto para aplicar os GPOs na máquina virtual durante o processo de logon. Agora, você pode ver o detalhamento de cada política aplicada de acordo com as CSEs (Extensão do Lado do Cliente) como uma dica de ferramenta na barra GPO. Para cada aplicação de política, o detalhamento exibe o status e o tempo gasto. Esta informação adicional facilita a solução de problemas e a remediação de problemas que envolvem alta duração de GPO. As durações de tempo no detalhamento representam apenas o tempo de processamento da CSE e não se somam ao tempo total do GPO. Este recurso está disponível no Delivery Controller versão 7 1808 e posterior. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Correções

As consultas de relatório personalizadas salvas durante o monitoramento não estão disponíveis após uma atualização do Cloud.

Outubro de 2018

Recursos novos e aprimorados

Aplicativos: Limite por máquina. Agora você pode limitar o número de instâncias de aplicativo por máquina. Este limite se aplica a todas as máquinas no Site. Este limite é um acréscimo ao limite de aplicativo existente para todos os usuários no Grupo de Entrega e ao limite por usuário. Essa capacidade está disponível apenas via PowerShell, não no Studio. Para obter detalhes, consulte Configurar limites de aplicativo.

Windows Server 2019. Agora você pode instalar VDAs para SO multi-sessão (anteriormente VDAs para SO de Servidor) em máquinas Windows Server 2019, conforme observado em Requisitos do sistema.

Setembro de 2018

Recursos novos e aprimorados

Administração Delegada. Com a Administração Delegada, você pode configurar as permissões de acesso que todos os seus administradores precisam, de acordo com sua função em sua organização. Para obter detalhes, consulte Administração Delegada. O monitoramento suporta a alocação de funções internas. As funções internas estão disponíveis com escopo total. Para obter mais informações sobre funções internas para monitoramento e como atribuí-las, consulte Funções de administrador delegado.

Registro de Configuração. O Registro de Configuração permite que os administradores acompanhem as alterações de configuração e as atividades administrativas. Para obter detalhes, consulte Registro de Configuração.

Vários cmdlets do PowerShell no SDK do PowerShell Remoto que estavam desabilitados anteriormente agora estão habilitados, para uso com o Registro de Configuração:

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore
- Log:ExportReport

Cache de Host Local. O Cache de Host Local agora está totalmente disponível. O Cache de Host Local permite que as operações de intermediação de conexão continuem quando um Cloud Connector em um local de recurso não consegue se comunicar com o Citrix Cloud. Para obter detalhes, consulte Cache de Host Local.

Citrix Provisioning. Para provisionar VDAs, agora você pode usar o Citrix Provisioning ou os Serviços de Criação de Máquinas existentes. Para obter informações do Citrix Provisioning específicas para o ambiente de nuvem, consulte Citrix Provisioning gerenciado pelo Citrix Cloud.

Correções

Em versões anteriores, ao usar o provisionamento sob demanda do Azure, todas as VMs eram excluídas quando desligadas. Agora, apenas as VMs agrupadas são excluídas. As VMs persistentes (dedicadas) não são excluídas quando desligadas.

Agosto de 2018

- **Novos nomes de produtos**

  Se você é cliente ou parceiro da Citrix há algum tempo, notará novos nomes em nossos produtos e nesta documentação do produto. Se você é novo neste produto Citrix, poderá ver nomes diferentes para um produto ou componente.

  Os novos nomes de produtos e componentes derivam do portfólio e da estratégia de nuvem em expansão da Citrix. Os artigos nesta documentação do produto usam os seguintes nomes.

  - **Citrix Virtual Apps and Desktops:** O Citrix Virtual Apps and Desktops oferece uma solução de aplicativo e desktop virtual, fornecida como um serviço de nuvem e como um produto local, dando aos funcionários a liberdade de trabalhar de qualquer lugar em qualquer dispositivo, ao mesmo tempo em que reduz os custos de TI. Entregue aplicativos Windows, Linux, web e SaaS ou desktops virtuais completos de qualquer nuvem: pública, local ou híbrida. O Virtual Apps and Desktops era anteriormente XenApp e XenDesktop.
  - **Citrix Workspace app:** O aplicativo Citrix Workspace incorpora a tecnologia Citrix Receiver existente e outras tecnologias de cliente Citrix Workspace. Ele foi aprimorado para oferecer mais recursos, a fim de proporcionar aos usuários finais uma experiência unificada e contextual, onde eles podem interagir com todos os aplicativos de trabalho, arquivos e dispositivos de que precisam para realizar seu melhor trabalho. Para obter mais informações, consulte esta postagem do blog.
  - **Citrix SD-WAN™:** O NetScaler SD-WAN, uma tecnologia crucial para nossos clientes e parceiros que estão transformando suas redes de filiais e WANs com tecnologia em nuvem, agora é Citrix SD-WAN.
  - **Citrix Secure Web Gateway™:** À medida que o portfólio de rede da Citrix se expande, temos o orgulho de oferecer nosso robusto serviço Citrix Secure Web Gateway, anteriormente conhecido como NetScaler Secure Web Gateway.
  - **Citrix Gateway:** Nosso robusto NetScaler® Unified Gateway, que permite acesso seguro e contextual aos aplicativos e dados de que você precisa para realizar seu melhor trabalho, agora é Citrix Gateway.
  - **Citrix Content Collaboration™ e Citrix Files para Windows:** Os recursos avançados de acesso, colaboração, fluxos de trabalho, gerenciamento de direitos e integração do ShareFile agora estão disponíveis no conjunto de componentes Citrix Content Collaboration em nosso Citrix Workspace seguro, contextual e integrado. O Citrix Files para Windows permite que você acesse seus arquivos do Content Collaboration

diretamente por meio de uma unidade mapeada, proporcionando uma experiência nativa do Windows Explorer.

- **Citrix Hypervisor**: A tecnologia do XenServer para infraestrutura de virtualização, baseada no hipervisor XenProject, agora é Citrix Hypervisor.

Aqui está um breve resumo:

É	ERA
Citrix Aplicativos Virtuais e Desktops	XenApp® e XenDesktop
Aplicativo Citrix Workspace	Incorpora Citrix Receiver e aprimoramentos extensivos
Citrix SD-WAN	NetScaler SD-WAN
Citrix Secure Web™ Gateway	NetScaler Secure Web Gateway
Citrix Gateway	NetScaler Unified Gateway
Citrix Content Collaboration	ShareFile
Citrix Files para Windows	ShareFile Desktop App, ShareFile Sync, ShareFile Drive Mapper
Citrix Hypervisor	XenServer
Citrix Provisioning	Citrix Provisioning Services

A implementação desta transição em nossos produtos e em sua documentação é um processo contínuo.

- O conteúdo do produto ainda pode conter nomes antigos. Por exemplo, você pode ver instâncias de nomes anteriores em texto de console, mensagens e nomes de diretórios/arquivos.
- É possível que alguns itens (como comandos e MSIs) continuem a manter seus nomes antigos para evitar quebrar scripts de clientes existentes.
- A documentação de produtos relacionados e outros recursos (como vídeos e postagens de blog) que estão vinculados à documentação deste produto ainda podem conter nomes antigos.

- Para Citrix Hypervisor: O novo nome é usado no site da Citrix e em materiais informativos de produtos a partir de setembro de 2018. Você também verá o novo nome nos consoles de administrador de alguns produtos Citrix, como Citrix Virtual Apps and Desktops. Os materiais de lançamento do produto XenServer e de documentação técnica continuam a usar o XenServer 7.x até o início de 2019.

Sua paciência durante esta transição é apreciada.

Para mais detalhes sobre nossos novos nomes, consulte `<https://www.citrix.com/about/citrix-product-guide/>`.

- **Alterações nos números de versão de produtos e componentes**

  A Citrix instala e gerencia a maioria dos componentes do Citrix Virtual Apps and Desktops, então você não precisará se preocupar com esses números de versão. No entanto, você poderá ver números de versão ao instalar Cloud Connectors e ao instalar ou atualizar VDAs em locais de recursos.

  Os números de versão de produtos e componentes do Citrix Virtual Apps and Desktops são exibidos no formato: **YYMM.*c.m.b***

  - YYMM = Ano e mês em que o produto ou componente foi lançado. Por exemplo, um lançamento de setembro de 2018 aparece como 1809.
  - c = Número da versão do Citrix Cloud para o mês.
  - m = Versão de manutenção (se aplicável).
  - b = Número da compilação. Este campo é exibido apenas na página Sobre do componente e no recurso do sistema operacional para remover ou alterar programas.

  Por exemplo, **Citrix Virtual Apps and Desktops 1809.1.0** indica que o componente foi lançado em setembro de 2018. Ele está associado à versão 1 do Citrix Cloud naquele mês e não é uma versão de manutenção. Algumas exibições mostram apenas o ano e o mês da versão: por exemplo, **Citrix Virtual Apps and Desktops 1809**.

  Em versões anteriores (7.18 e anteriores), os números de versão eram exibidos no formato: 7.*versão*, onde a versão incrementava em um a cada lançamento. Por exemplo, o lançamento do VDA após o XenApp e XenDesktop 7.17 foi 7.18. Versões anteriores (7.18 e anteriores) não serão atualizadas com o novo formato de numeração.

- **Descontinuação das versões TLS.** Para melhorar a segurança do serviço Citrix Virtual Apps and Desktops, a Citrix bloqueará qualquer comunicação via Transport Layer Security (TLS) 1.0

e 1.1, a partir de December 31, 2018. Para detalhes, consulte Descontinuação das versões TLS.

- **Ambiente de virtualização do Google Cloud Platform.** O serviço Citrix Virtual Apps and Desktops oferece suporte à capacidade de reiniciar manualmente VMs do Virtual Apps and Desktops no Google Cloud Platform (GCP). Para obter mais informações, consulte Ambientes de virtualização do Google Cloud Platform.

Julho de 2018

- **Exportação de dados de Filtros.** Agora você pode exportar dados de monitoramento em tempo real na guia **Monitor** > **Filtros** para arquivos no formato CSV. O recurso de exportação está disponível nas páginas de Filtros de Máquinas, Sessões, Conexões e Instâncias de Aplicativos. Você pode selecionar um filtro personalizado predefinido ou selecionar critérios de filtro adequados, escolher as colunas necessárias na tabela e exportar os dados. Dados de até 100.000 registros podem ser exportados. Os arquivos CSV exportados fornecem uma visão abrangente dos dados em tempo real e ajudam a facilitar a análise de grandes conjuntos de dados.

Junho de 2018

- **Conexões do Azure Resource Manager.** No assistente de criação de conexão do Studio, a seleção do ambiente Azure na página **Conexão** inclui todas as Nuvens Azure válidas para sua assinatura Azure. A disponibilidade geral para Azure US Government Cloud e Azure Germany Cloud substitui as versões de visualização desses dois ambientes em versões anteriores.

Maio de 2018

- **Azure Quick Deploy.** Quando seu local de recurso usa máquinas do Azure Resource Manager para entregar aplicativos e desktops, agora você pode escolher um método de implantação:
  - Configuração Completa: Este método existente usa o console de gerenciamento do Studio, que o guia na criação de um catálogo de máquinas e, em seguida, na criação de um Grupo de Entrega.
  - Azure Quick Deploy: Esta nova opção oferece uma interface mais simples que proporciona uma implantação mais rápida de aplicativos e desktops.
- **Link do Citrix Health Assistant.** A página Detalhes da Máquina de uma máquina não registrada no console de Monitoramento agora contém um botão **Health Assistant**. Atualmente, o botão vincula a Solucionar problemas de máquinas e ao artigo da Central de

Conhecimento, Citrix Health Assistant - Solucionar problemas de registro de VDA e inicialização de sessão onde você pode baixar a ferramenta. O Citrix Health Assistant é uma ferramenta para solucionar problemas de configuração em VDAs não registrados. A ferramenta automatiza várias verificações de saúde para identificar possíveis causas raiz para problemas comuns de registro de VDA, inicialização de sessão e configuração de redirecionamento de fuso horário.

- **Detalhamento da Sessão Interativa.** No console de monitoramento, o painel **Visualização de Detalhes do Usuário > Duração do Logon** agora inclui informações sobre o estágio de **Sessão Interativa** do processo de logon. Para fornecer uma solução de problemas e remediação mais granular desta fase do logon, a **Sessão Interativa** agora tem três subfases: **Pre-userinit**, **Userinit** e **Shell**. Nesta versão, passar o mouse sobre **Sessão Interativa** exibe uma dica de ferramenta mostrando as subfases e um link para a documentação. Para uma descrição das subfases e como melhorar o desempenho de cada fase, consulte Diagnosticar problemas de logon do usuário.

Março de 2018

- **Previsão de instâncias de aplicativo (Recurso de visualização).** Este é o primeiro recurso de monitoramento baseado em análise preditiva. Prever padrões de uso de recursos é importante para que os administradores organizem os recursos e o número necessário de licenças em cada recurso. O recurso de previsão de instâncias de aplicativo indica o número de instâncias de aplicativo hospedadas que provavelmente serão iniciadas por Site ou Grupo de Entrega ao longo do tempo. Algoritmos de aprendizado de máquina baseados em modelos de dados criados com dados históricos existentes são usados para fazer a previsão. O nível de tolerância indica a qualidade da previsão.

  Para obter mais informações, consulte Previsão de instâncias de aplicativo no Monitor. Envie seu feedback sobre a utilidade e usabilidade deste recurso no fórum de discussão do Citrix Cloud.

- **APIs de Grupos de Entrega - Visualização**

  A Visualização das APIs de Grupos de Entrega fornece um conjunto de APIs REST que você pode usar para automatizar o gerenciamento de Grupos de Entrega. O conjunto completo de APIs disponíveis pode ser visualizado e testado na documentação da API do Citrix Cloud em `<https://developer.cloud.com/>`.

- **Autenticação do Web Studio**

O console de gerenciamento de serviço no Citrix Cloud agora usa um token de portador para autenticar clientes. O token de portador é necessário para autenticar o acesso à API REST de Delivery Groups.

- **Acessar dados do Monitor Service usando a API OData Versão 4 (recurso de visualização)**

  Você pode criar seus painéis de monitoramento e relatórios personalizados com base nos dados do Monitor Service usando o endpoint OData V.4. O OData V.4 é baseado na API Web ASP .Net e oferece suporte a consultas de agregação. Use seu nome de usuário do Citrix Cloud e o token de portador para acessar os dados com o endpoint V4. Para obter mais informações e exemplos, consulte Acessar dados do Monitor Service usando o endpoint OData v4 no Citrix Cloud.

  Compartilhe seus comentários sobre a utilidade desse recurso no fórum de discussão do Citrix Cloud.

Correções

- Você pode renomear, mover e excluir pastas de aplicativos.

Janeiro de 2018

- **Verificação de licença RDS.** A criação de catálogos de máquinas contendo máquinas com SO Windows Server agora inclui uma verificação automática de licença RDS. Quaisquer problemas de licença RDS encontrados são exibidos, para que você possa tomar as medidas apropriadas para evitar uma interrupção no serviço. Para obter detalhes, consulte Criar catálogos de máquinas.
- **Acesso ao console da máquina a partir do Monitor.** O painel Detalhes da Máquina do Monitor agora fornece acesso aos consoles de máquinas hospedadas no hipervisor XenServer versão 7.3. Agora você pode solucionar problemas em VDAs diretamente do Monitor. Para obter mais informações, consulte Acesso ao console da máquina em Solucionar problemas de máquinas.

Dezembro de 2017

Recursos novos e aprimorados

- **Citrix Workspace.** O Citrix Workspace agora está disponível para **novos** clientes do serviço XenApp e XenDesktop. Para obter mais informações, consulte Configuração do Workspace.

- **Análise de Aplicativos.** Agora você pode analisar e monitorar o desempenho de aplicativos de forma eficiente com a nova página Análise de Aplicativos, disponível na guia **Monitor** > **Aplicativos**. A página fornece uma visão consolidada da integridade e do uso de todos os aplicativos publicados em seu Site. Ela mostra métricas como o número de instâncias por aplicativo e falhas e erros associados aos aplicativos publicados. Esse recurso requer VDAs Versão 7.15 ou posterior.

  Para obter mais informações, consulte a seção Análise de Aplicativos em Monitor.

Novembro de 2017

Recursos novos e aprimorados

- **Cache de Host Local.** O Cache de Host Local permite que as operações de intermediação de conexão continuem quando um Cloud Connector em um local de recurso não consegue se comunicar com o Citrix Cloud. Para obter detalhes, consulte Cache de Host Local.
- **Discos Gerenciados do Azure.** Os Discos Gerenciados do Azure agora são usados por padrão para VMs provisionadas por MCS em ambientes do Azure Resource Manager. Opcionalmente, você pode usar contas de armazenamento convencionais. Para obter detalhes, consulte Ambientes de virtualização do Microsoft Azure Resource Manager.
- **Administrador de help desk.** Ao gerenciar administradores de serviço para uma conta de cliente do Citrix Cloud, agora você tem uma nova opção: Administrador de Help Desk. Um administrador de help desk pode acessar as funções de Monitor no serviço. Para obter detalhes, consulte Gerenciar.

Correções

- Agora você pode usar o assistente do console de gerenciamento de serviço para criar um catálogo de máquinas do Acesso Remoto para PC. Em versões anteriores, você precisava usar um cmdlet do PowerShell para criar um catálogo (conforme documentado em CTX220737). Em seguida, você precisava retornar ao console de gerenciamento para criar um Grupo de Entrega. Agora, você cria o catálogo e o Grupo de Entrega sequencialmente no console de gerenciamento.
- Os catálogos criados por MCS podem usar contas de máquina existentes do Active Directory.
- Ao monitorar uma implantação, a rolagem em uma tabela classificada de **Tendências > Sessões** exibe resultados precisos.

Mais informações

- Problemas conhecidos.
- Para obter informações sobre software de terceiros incluído no serviço, consulte Notificações de terceiros.

Problemas conhecidos

O Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™) apresenta os seguintes problemas conhecidos:

- A atualização de uma imagem mestre habilitada para vTPM para um catálogo de máquinas não persistentes do MCS por meio de uma conexão Nutanix AHV Prism Central aciona uma recriação de VM que pode invalidar as reservas de DNS e exigir um novo registro para softwares que utilizam endereços MAC para licenciamento.
- Ao usar um perfil de máquina que possui várias interfaces de rede (NICs) com Rede Acelerada habilitada, certifique-se de que o tamanho da VM selecionado suporte Rede Acelerada em todas as NICs. Alguns tamanhos de VM do Azure (por exemplo, Standard_D2ads_v5) restringem a Rede Acelerada a uma única NIC. Se o perfil da máquina habilitar a Rede Acelerada em mais NICs do que o tamanho da VM permite, as máquinas falharão ao ligar com o erro `VmSizeRestrictedToSingleNicWithAcceleratedNetworkingEnable`. Para resolver isso, selecione um tamanho de VM que suporte Rede Acelerada em várias NICs ou atualize o perfil da máquina para habilitar a Rede Acelerada em apenas uma NIC.
- Adicionar um grande lote de VMs a um catálogo MCS usando uma conexão de host Nutanix AHV Prism Central pode falhar com um erro `OutOfMemory`. Para evitar isso, reduza o número de VMs criadas em um único lote. Recomendamos adicionar no máximo 10 VMs por vez.
- Os custos por hora para certas SKUs de Instância do Azure Windows (por exemplo, `Standard_DS*{_}v2{_}*`) são exibidos como **Indisponível** no Studio. Isso ocorre porque nosso recurso de custo depende da API de Preços de Recursos do Azure pública, e esta API, por design, não fornece mais informações de preços para certos dados de medidor que ela descontinuou de seus próprios relatórios. Essa limitação afeta a exibição dos preços de varejo e efetivos para as SKUs de Instância do Windows dentro do sistema.
- Se o UPN do usuário do Azure contiver um ponto como o vigésimo caractere, o VDA do Windows Server não conseguirá criar uma conta de usuário local.
- Ao criar um catálogo de máquinas MCS em um ambiente de virtualização Red Hat OpenShift, você não pode usar uma imagem mestre e um perfil de máquina que tenham tipos de sistema

operacional diferentes. Isso se deve à forma como o Red Hat OpenShift gerencia cada tipo de SO. Portanto, usar uma VM Windows como imagem mestre com uma VM não Windows (exemplo, Linux) como perfil de máquina, ou vice-versa, não é suportado.

- Atualmente, as VMs criadas usando `InstanceType` não são suportadas como imagem mestre.
- Quando o metainstalador é usado para instalar os componentes do Citrix Virtual Apps and Desktops em uma máquina executando o Windows Server 2025, os eventos MsiInstall não são gravados nos logs de eventos.
- Depois de criar um backup e navegar para a guia **Componentes** desse backup selecionado, você verá dados vazios para um componente que possui um recurso depois de clicar em **Exibir membros do componente**.
- Ao tentar restaurar conexões de hospedagem AWS, Azure, GCP e XenServer®, a **Contagem de restauração** na página **Progresso da restauração** é **1** e exibe apenas o resultado da ação de restauração do XenServer.
- Depois de criar um backup, a contagem de componentes de **Conexões de Hospedagem** na página **Progresso do backup** é exibida como **0**.
- Em um ambiente VMware hospedado na AWS, a criação do catálogo de máquinas MCS falha se a imagem mestre estiver com vTPM habilitado. Esse problema afeta todas as versões do Citrix Virtual Apps and Desktops e é devido a um problema no ambiente VMware. Para obter assistência, entre em contato com o suporte VMware.
- Se você usa os Serviços de Domínio do Microsoft Entra: Os UPNs de logon do usuário final devem conter o nome de domínio que foi especificado ao habilitar os Serviços de Domínio do Microsoft Entra ID. Os logons não podem usar UPNs para um domínio personalizado que você cria, mesmo que esse domínio personalizado seja designado como primário.

Para problemas relacionados aos VDAs atuais, consulte Problemas conhecidos.

Descontinuações e remoções

Este artigo fornece um aviso antecipado sobre os recursos do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) que estão sendo descontinuados, para que você possa tomar decisões de negócios oportunas. A Citrix monitora o uso e o feedback dos clientes para determinar quando os recursos são retirados. Os anúncios podem mudar em versões subsequentes e podem não incluir todos os recursos ou funcionalidades descontinuados. Para obter detalhes sobre o suporte ao ciclo de vida do produto, consulte o artigo Política de Suporte ao Ciclo de Vida do Produto.

Nota:

As descontinuações e remoções do Citrix Virtual Apps and Desktops são descritas em seu próprio artigo Descontinuação.

Descontinuações e remoções

A lista a seguir mostra os recursos do Citrix DaaS™ que foram descontinuados ou removidos.

- Itens *descontinuados* não são removidos imediatamente. A Citrix® continua a suportá-los, mas eles serão removidos em uma versão futura.
- Itens *removidos* são removidos ou não são mais suportados no Citrix DaaS. As datas em **negrito** indicam as atualizações mais recentes.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Suporte para o plug-in de terceiros HPE Moonshot Machine Manager	Maio de 2024	-	Use o plug-in HPE Moonshot gerenciado pela Citrix
A coluna **Last Boot Time (UTC)** no Studio e o campo **LastBootTime** nas respostas de **Get-ProvVM** e **Get-ProvVMDetails**	Julho de 2026	-	-
Opção da interface do usuário do Studio para	Abril de 2026		Migrar para o modelo de

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
infraestrutura completa do App-V			administrador único do App-V
Substituições de licença por grupo de entrega (licenciamento de vários tipos)	Abril de 2026	O Citrix DaaS usa apenas configurações de licença no nível do site. As substituições de grupo de entrega são ignoradas e a etapa **Atribuição de Licença** nos assistentes Criar e Editar Grupo de Entrega é removida. Para obter mais informações, consulte Licenças.	
Suporte para `Get-BrokerMachine`	Julho de 2025	Use `Get-BrokerMachineV2`	
Suporte para `$XDSDKAuth` para autenticação SDK	Junho de 2025	Junho de 2025	Executar `Get-XDAuthentication -ProfileName WindowsCurrentUser`

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Suporte para os seguintes comandos PowerShell `-AcctADAccount` • New-AcctADAccount • Add-AcctADAccount • Update-AcctADAccount • Remove-AcctADAccount • Unlock-AcctADAccount • Get-AcctADAccount	Dezembro de 2024		Usar os comandos PowerShell -AcctIdentity • New-AcctIdentity • Add-AcctIdentity • Update-AcctIdentity • Remove-AcctIdentity • Unlock-AcctIdentity • Get-AcctIdentity
Suporte para o comando PowerShell `Repair-AcctADAccount`	Dezembro de 2024		Use os seguintes comandos

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
			• `Repair-AcctIdentity`: Para reparar contas de identidade sem alterar o estado atual delas. Isso pode reparar contas de identidade existentes em uso para VMs provisionadas existentes. Por exemplo, atributos `repair userCertificate` para contas de identidade híbridas do Microsoft Entra. O `Repair`

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
			`identity info` (incluindo senha da máquina/ par de chaves de confiança) para contas de identidade unidas ao AD. • `Reset-AcctIdentity`: Para redefinir contas de identidade para os estados iniciais (Por exemplo, de corrompidas para disponíveis). Isso pode colocar quaisquer contas de

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
			identidade corrompidas de volta ao pool como contas de identidade disponíveis.
Suporte para o comando PowerShell `-ResetIdentityInfo`	Outubro de 2024		Use `-Recreate` para recriar o disco de identidade. Para obter informações, consulte Reparar as informações de identidade de contas de computador ativas.
Suporte para configurar o cache de write-back de E/S do MCS para incluir apenas um cache de disco e nenhum cache de memória	Fevereiro de 2024	Janeiro de 2025	NA

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Suporte para catálogos do Azure criados antes do recurso de provisionamento sob demanda (catálogos "legados")	Fevereiro de 2024		Recrie as VMs de catálogo legadas do Azure. Os catálogos são provisionados sob demanda e ajudam a economizar custos de armazenamento.
Suporte para Citrix Connector 3.1 para System Center Configuration Manager	Dezembro de 2023	Agosto de 2025	Faça a atualização da imagem ou do aplicativo manualmente.
Suporte para usar uma imagem mestre em uma região diferente da região onde o catálogo é criado	Dezembro de 2023		Use a Galeria de Computação do Azure para replicar a imagem mestre para a região necessária.
Suporte para worker de volume AWS	Novembro de 2023	Junho de 2025	Use o upload e download direto de disco. Consulte Upload e download direto de disco.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Suporte para `Leave user management to Citrix Cloud` usado na criação de grupos de entrega	Setembro de 2023	Setembro de 2023	
Suporte para `AwsCaptureInstanceProperties` usado em ambientes AWS	Agosto de 2023		Use um perfil de máquina. Consulte Criar um catálogo usando um perfil de máquina.
Suporte para VMware vSphere 6.7		Junho de 2023	Use versões superiores para VMware vSphere.
Comando PowerShell `Schedule-ProvVMUpdate`	Abril de 2023		Use o comando `Set-ProvVMUpdateTimeWindow`.
Comando PowerShell `Request-ProvVMUpdate`	Abril de 2023		Use o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`.

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
`Cancel-ProvVMUpdate` comando PowerShell	Abril de 2023		Use o comando `Clear-ProvVMUpdateTimeWindow`.
Parâmetro `DedicatedTenancy` usado no comando `New-ProvScheme`	Março de 2023		Use o parâmetro `TenancyType`.
Disco não gerenciado para criar VM no ambiente Azure	Junho de 2022		
Suporte para quatro comandos específicos da AWS: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` e `Grant-HypSecurityGroupIngress`	Maio de 2022		

ITEM	DESCONTINUAÇÃO ANUNCIADA NA VERSÃO	REMOVIDO NA VERSÃO	ALTERNATIVA
Parâmetro `StorageAccountType` usado em ambientes Azure	Abril de 2022		Use `StorageType`.
Console herdado (console baseado em MMC)	Julho de 2021	Novembro de 2021	Use **DaaS > Gerenciar** para acessar toda a gama de ações de configuração e gerenciamento.
Implantação Rápida do Azure	Setembro de 2020		Use Implantação Rápida.
Capacidade de importar dispositivos de destino do Citrix Provisioning para criar catálogos no Citrix Studio.	Agosto de 2020	Fevereiro de 2021	Use o Assistente de Exportação de Dispositivos do Citrix Provisioning para enviar VMs do Citrix Provisioning para Delivery Controllers/ MCS para criação de catálogo. Consulte Assistente de Exportação de Dispositivos.

Recursos em prévia

Recursos em prévia estão disponíveis para uso em ambientes de não produção ou produção limitada, e para dar aos clientes a oportunidade de compartilhar feedback. A Citrix® não aceita casos de suporte para recursos em prévia, mas agradece o feedback para melhorá-los. A Citrix pode agir com base no feedback, considerando sua gravidade, criticidade e importância.

Lista de recursos em prévia

A tabela a seguir lista os recursos em prévia.

TÍTULO	FORMULÁRIO DE HABILITAÇÃO (CLIQUE NO ÍCONE)	FORMULÁRIO DE FEEDBACK (CLIQUE NO ÍCONE)
Integração do Citrix com o Azure Local para cargas de trabalho Linux	☐	NA
Integração do Secure Private Access com o Monitor	NA	NA
Registro de VMs não persistentes unidas ao Hybrid Entra ID no Microsoft Intune	☐	NA
Suporte a Múltiplas Versões VUS	NA	NA

Integração do Citrix com o Azure Local para cargas de trabalho Linux

O Azure Local é uma solução de infraestrutura hiperconvergente (HCI) que conecta o sistema local ao Azure para serviços baseados em nuvem, monitoramento e gerenciamento.

Com este recurso, o MCS oferece suporte ao Azure Local como uma nova plataforma e, portanto, oferece suporte a:

- Provisionamento de VMs Linux habilitadas para Azure Arc no Azure Local.
- Gerenciamento de energia de VMs Linux criadas no Azure Local.

Para obter mais informações, consulte Integração do Citrix com o Azure Local para cargas de trabalho Linux.

Integração do Secure Private Access com o Monitor

Esta prévia permite que o administrador monitore e solucione problemas de todas as sessões do Secure Private Access no Monitor.

As ações disponíveis incluem a visualização dos detalhes do seguinte:

- Sessões ativas do Secure Private Access para um usuário em pop-up Selecionar uma Sessão > guia Sessões Ativas
- Enumerações falhas ou bloqueadas do Secure Private Access e inicializações de aplicativos falhas em pop-up Selecionar uma Sessão > guia Acesso Negado
- Visualização de detalhes de sessão e aplicativo para inicializações de aplicativos ativas e com falha, bem como para enumerações com falha e bloqueadas

Para obter mais informações, consulte a página de integração do Secure Private Access com o Monitor (Visualização).

Registro de VMs não persistentes unidas ao Hybrid Entra ID no Microsoft Intune

Com esta visualização, agora você pode registrar VMs não persistentes unidas ao Hybrid Entra ID no Microsoft Intune (com o Configuration Manager) para gerenciamento conjunto. Este recurso se aplica a VMs não persistentes de sessão única e multi-sessão e em todos os hipervisores e serviços de nuvem, garantindo um gerenciamento uniforme de dispositivos em toda a sua infraestrutura. Para usar o recurso, a versão do VDA deve ser 2407 ou posterior. Para obter mais informações, consulte Registro de VMs não persistentes unidas ao Hybrid Entra ID no Microsoft Intune.

Suporte a Múltiplas Versões do VUS

Anteriormente, o VUS permitia apenas atualizações para a versão mais recente do VDA lançada em cada Trilha de Atualização. Este novo recurso de visualização técnica permite que você atualize para versões novas e lançadas anteriormente do VDA. Este recurso é compatível com atualizações de nível de catálogo e atualizações de VDA de nível de máquina individual. Para obter mais informações, consulte Suporte a Múltiplas Versões do VUS.

Da visualização à disponibilidade geral (GA)

- Co-gerenciamento de locatários para DaaS multilocatário CSP
- Integração com Nutanix Prism Central no AHV
- Gerenciamento de imagens
- Suporte para criar e gerenciar VMs confidenciais do Azure usando a Configuração Completa

- Suporte para plug-in HPE Moonshot gerenciado pela Citrix
- Hibernação do Azure
- Conjuntos de políticas
- Economia de custos
- Diagnosticar sessões de usuário históricas
- Monitoramento de infraestrutura
- Política de infraestrutura
- Monitorar várias instâncias do Citrix DaaS

Requisitos do sistema

Introdução

Os requisitos do sistema para componentes que não são abordados aqui (como o aplicativo Citrix Workspace™ e o Citrix Provisioning™) são descritos em suas respectivas documentações.

Recomendações específicas para dimensionar VMs que fornecem desktops e aplicativos não podem ser fornecidas devido à natureza complexa e dinâmica das ofertas de hardware. Cada implantação tem necessidades exclusivas. Geralmente, o dimensionamento de uma VM é baseado no hardware e não nas cargas de trabalho do usuário (exceto para RAM; você precisa de mais RAM para aplicativos que consomem mais). O Citrix Tech Zone contém as orientações mais recentes sobre o dimensionamento de VDA.

> **Importante:**

> As versões do VDA mencionadas neste artigo estão sujeitas ao ciclo de vida do produto Citrix. Para obter mais informações, consulte a Matriz de Produtos no site da Citrix.

> Para obter mais informações sobre como usar VDAs LTSR com o Citrix DaaS, consulte CTX205549.

> **Lembre-se:** Em uma implantação do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™), você não precisa instalar ou gerenciar os componentes principais (Delivery Controllers, o banco de dados do site ou os consoles de gerenciamento e monitoramento). Para obter orientações sobre a instalação do Virtual Delivery Agent (VDA), consulte:

- Instalar VDAs
- Instalar VDAs usando a linha de comando.

Cloud Connectors

Para obter detalhes, consulte Detalhes Técnicos do Cloud Connector.

Validação de conectividade do hipervisor

Para oferecer suporte à transição do gerenciamento de hipervisor (XenServer, VMware, AWS) dos Cloud Connectors para o Cloud Delivery Controller, o Citrix DaaS fornece um mecanismo automatizado de validação de conectividade. Essa ferramenta verifica se o serviço pode alcançar os endpoints do seu local de recurso sem impactar os ambientes de produção.

Validação pré-migração

Antes que o plugin seja movido para a nuvem, o sistema realiza um proteger de integridade no **Modo de Validação** para identificar lacunas de configuração em:

- **Rede:** Regras de firewall, resolução de DNS e roteamento.
- **Segurança:** Confiança de certificado SSL/TLS e handshakes.
- **Autenticação:** Validade das credenciais do novo contexto de execução.

Relatórios acionáveis

Os resultados da validação são exibidos diretamente na **Studio UI** e nas **Verificações de Prontidão para Migração**. Se uma verificação falhar, o sistema fornece detalhes de erro específicos (por exemplo, tempos limite de conexão ou incompatibilidades de certificado) por meio de:

- **Indicadores de Status de Integridade:** Visibilidade em tempo real no console de gerenciamento. Consulte https://docs.citrix.com/pt-br/citrix-daas/manage-deployment/vda-health-checks#run-health-checks-for-vdas
- **Logs de Eventos:** Registros detalhados para remediação pré-migração.
- **Alertas Pós-Migração:** Monitoramento contínuo de problemas de configuração relacionados ao NGS.

VDAs em um ambiente Azure

Sistemas operacionais suportados:

- Windows 11 multi-sessão
- Windows 11 sessão única
- Windows 10 multi-sessão
- Windows 10 sessão única
- Windows Server 2025

- Windows Server 2022 (requer no mínimo VDA 2106)
- Windows Server 2019
- Windows Server 2016

Todos os VDAs que não atingiram o fim da vida útil são suportados para uso com o Citrix DaaS. Para VDAs LTSR, recomendamos usá-los com a Atualização Cumulativa mais recente. Para obter mais informações sobre o ciclo de vida dos VDAs, consulte Citrix Product Matrix.

O Windows Server 2012 R2 é suportado apenas com o VDA 1912 (e CUs posteriores).

O Windows Server requer Microsoft RDS licensing.

Para obter informações sobre o Azure Virtual Desktop, consulte a documentação da Microsoft.

VDAs em Instâncias Gerenciadas do Amazon WorkSpaces Core

Sistemas operacionais suportados:

- Windows 11 de sessão única
- Windows 10 de sessão única
- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Ubuntu Server 24.04 LTS
- Debian 12

VDA para SO de sessão única

As informações a seguir se aplicam à versão mais recente do VDA.

Sistemas operacionais suportados:

- Windows 11
- Windows 10
    - Para suporte a edições, consulte CTX224843. Esse artigo também contém links para problemas conhecidos da Citrix com as versões suportadas do Windows.

  - O redirecionamento de composição da área de trabalho e o modo gráfico herdado não são suportados no Windows 10.

Requisitos:

- O Microsoft .NET Framework 4.8 é instalado automaticamente, se ele (ou uma versão posterior) ainda não estiver instalado.
- Microsoft Visual C++ 2015-2019 Redistributable.
  - Se a máquina contiver uma versão anterior desse tempo de execução (como 2015-2017), o instalador Citrix® o atualiza.
  - Se a máquina contiver uma versão anterior a 2015, a Citrix instala a versão mais recente em paralelo.

O Acesso Remoto a PC usa este VDA, que você instala em PCs físicos de escritório. Este VDA oferece suporte a Secure Boot para Citrix Virtual Desktops™ Acesso Remoto a PC.

Vários recursos de aceleração multimídia (como HDX™ MediaStream Windows Media Redirection) exigem que o Microsoft Media Foundation esteja instalado na máquina onde você instala o VDA. Se a máquina não tiver o Media Foundation instalado, os recursos de aceleração multimídia não serão instalados e não funcionarão. Não remova o Media Foundation da máquina após instalar o software Citrix. Caso contrário, os usuários não conseguirão fazer logon na máquina. Na maioria das edições de SO de desktop Windows suportadas, o suporte ao Media Foundation já está instalado e não pode ser removido. No entanto, as edições N não incluem certas tecnologias relacionadas a mídia. Você pode obter esse software da Microsoft ou de terceiros.

Mais informações:

- Para obter informações sobre o VDA para Linux, consulte a documentação do produto Linux Virtual Delivery Agent.
- Para usar o recurso VDI de servidor, você pode usar a interface de linha de comando para instalar um VDA de sessão única em uma máquina Windows Server suportada. Consulte Server VDI para obter orientação.
- Para obter informações sobre como instalar um VDA em uma máquina mais antiga, consulte Sistemas operacionais anteriores.
- Consulte também VDAs em um ambiente de Área de Trabalho Virtual do Azure.

VDA para SO multissessão

As informações a seguir se aplicam à versão mais recente do VDA.

Sistemas operacionais suportados:

- Windows Server 2025 (requer VDA 2407 mínimo)
- Windows Server 2022 (requer VDA 2106 mínimo)
- Windows Server 2019, edições Standard e Datacenter
- Windows Server 2016, edições Standard e Datacenter
- Windows 11
- Windows 10 (64 bits) todas as versões suportadas

O instalador implanta automaticamente os seguintes requisitos:

- O Microsoft .NET Framework 4.8 é instalado automaticamente, se ele (ou uma versão posterior) ainda não estiver instalado.
- Microsoft Visual C++ 2015-2019 Redistributable.
    - Se a máquina contiver uma versão anterior desse tempo de execução (como 2015-2017), o instalador da Citrix a atualizará.
    - Se a máquina contiver uma versão anterior a 2015, a Citrix instalará a versão mais recente em paralelo.

O instalador instala e habilita automaticamente os serviços de função dos Serviços de Área de Trabalho Remota, se eles ainda não estiverem instalados e habilitados. Isso aciona uma reinicialização.

Vários recursos de aceleração multimídia (como HDX MediaStream Windows Media Redirection) exigem que o Microsoft Media Foundation seja instalado na máquina onde você instala o VDA. Se a máquina não tiver o Media Foundation instalado, os recursos de aceleração multimídia não serão instalados e não funcionarão. Não remova o Media Foundation da máquina após instalar o software Citrix. Caso contrário, os usuários não conseguirão fazer logon na máquina. Na maioria das versões do Windows Server, o recurso Media Foundation é instalado por meio do Gerenciador do Servidor. No entanto, as edições N não incluem certas tecnologias relacionadas a mídia. Você pode obter esse software da Microsoft ou de terceiros.

Se o Media Foundation não estiver presente no VDA, estes recursos multimídia não funcionarão:

- Redirecionamento de Flash

- Redirecionamento de Mídia do Windows
- Redirecionamento de Vídeo HTML5
- Redirecionamento de Webcam HDX RealTime

Mais informações:

- Para obter informações sobre o VDA para Linux, consulte os artigos Linux Virtual Delivery Agent.
- Para obter informações sobre a instalação de um VDA em um sistema operacional Windows que não é mais compatível, consulte Sistemas operacionais anteriores.
- Consulte também VDAs em um ambiente de Área de Trabalho Virtual do Azure.

Hosts / recursos de virtualização

Os seguintes recursos de host/virtualização (listados em ordem alfabética) são compatíveis. Quando aplicável, as versões *principal.secundária* são compatíveis, incluindo atualizações para essas versões. CTX131239 contém as informações de versão mais atuais do hipervisor, além de links para problemas conhecidos.

- **Amazon Web Services (AWS)**
  - Você pode provisionar aplicativos e desktops em sistemas operacionais de servidor Windows compatíveis.
  - O Amazon Relational Database Service (RDS) não é compatível.

  Para obter mais informações, consulte Ambientes de nuvem AWS.
- **Instâncias Gerenciadas do Amazon WorkSpaces Core**

  Para obter mais informações, consulte Ambientes de nuvem AWS.
- **XenServer (anteriormente Citrix Hypervisor™)**

  CTX131239 contém informações da versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte Ambientes de virtualização XenServer.
- **Google Cloud Platform**

  Para obter mais informações, consulte Ambientes do Google Cloud e Introdução ao Citrix DaaS no Google Cloud.
- **HPE Moonshot**

Para obter mais informações, consulte ambientes de virtualização HPE Moonshot.

- **Microsoft Azure Resource Manager**

  Para obter mais informações, consulte ambientes de nuvem do Microsoft Azure Resource Manager.

- **Microsoft System Center Virtual Machine Manager**

  Inclui qualquer versão do Hyper-V que possa ser registrada nas versões compatíveis do System Center Virtual Machine Manager.

  CTX131239 contém informações da versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte ambientes de virtualização do Microsoft System Center Virtual Machine Manager.

- **Nutanix Prism Central no AHV**

  Para obter mais informações, consulte Nutanix Prism Central no AHV.

- **Nutanix Acropolis com Prism Element**

  CTX131239 contém informações da versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte Nutanix Prism Element no AHV.

- **NC2 para plug-in do Nutanix AHV Prism Central gerenciado pelo Citrix**

  Para obter mais informações, consulte Nutanix AHV Prism Central.

- **NC2 para Nutanix Prism Element**

  Para obter mais informações, consulte NC2 para Nutanix Prism Element.

- **Red Hat OpenShift**

  Para obter mais informações, consulte ambientes de virtualização Red Hat OpenShift.

- **VMware Cloud on AWS**

  CTX131239 contém informações da versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte VMware Cloud on Amazon Web Services (AWS).

- **Azure VMware Solution (AVS)**

  CTX131239 contém informações da versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte integração do Azure VMware Solution (AVS).

- **Google Cloud VMware Engine**

  CTX131239 contém informações da versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte Google Cloud VMware Engine.

- **VMware vSphere(vCenter + ESXi)**

  Não há suporte para a operação do vSphere vCenter Linked Mode.

  CTX131239 contém informações da versão atual, além de links para problemas conhecidos.

  Para obter mais informações, consulte VMware virtualization environments.

> **Nota:**
>
> Você não deve instalar o software VDA em nenhum servidor Citrix DDC ou StoreFront. O VDA deve ser um sistema autônomo. A instalação de vários componentes em uma única VM é permitida apenas ao desenvolver uma prova de conceito ou ao publicar o console de administração do Studio apenas para administradores. Neste caso, você deve garantir que usuários não administradores não tenham acesso às VMs DDC/StoreFront.

Níveis funcionais do Active Directory

Os seguintes níveis funcionais para a floresta e o domínio do Active Directory são suportados:

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2

Para obter mais informações sobre o Active Directory, consulte Active Directory joined.

Tecnologias HDX

Para suporte e requisitos específicos de recursos HDX, consulte HDX.

Servidor de Impressão Universal

O Servidor de Impressão Universal compreende componentes de cliente e servidor. O componente UpsClient está incluído na instalação do VDA. Você instala o componente UpsServer

em cada servidor de impressão onde residem impressoras compartilhadas que você deseja provisionar com o Citrix Universal™ Print Driver em sessões de usuário.

O componente UpsServer é suportado em:

- Windows Server 2025
- Windows Server 2019
- Windows Server 2016

Requisitos:

- Microsoft .NET Framework 4.8 (mínimo)
- Microsoft Visual C++ 2015-2022 Redistributable.
    - Se a máquina contiver uma versão anterior desse tempo de execução (como 2015-2017), o instalador Citrix a atualizará.
    - Se a máquina contiver uma versão anterior a 2015, o Citrix instalará a versão mais recente em paralelo.

Para VDAs de múltiplas sessões, a autenticação do usuário durante as operações de impressão exige que o Universal Print Server esteja associado ao mesmo domínio que o VDA.

Pacotes de componentes de cliente e servidor autônomos também estão disponíveis para download.

Para obter mais informações, consulte Provisionar impressoras.

Conectividade de serviço

Consulte Requisitos de sistema e conectividade para obter informações sobre a conexão com a Internet. Essas informações incluem requisitos comuns à maioria dos serviços do Citrix Cloud, além de requisitos específicos do Citrix DaaS.

Outros

- O Microsoft Group Policy Management Console (GPMC) é necessário se você armazenar informações de política do Citrix no Active Directory em vez do banco de dados de configuração do site. A máquina na qual você instala `CitrixGroupPolicyManagement_x64.msi` deve ter o tempo de execução do Visual Studio 2015 instalado. Para obter mais informações, consulte a documentação da Microsoft.

- Este produto oferece suporte às versões 3 a 5 do PowerShell.
- Para componentes e recursos do produto que você pode instalar em Servidores Windows, as instalações do Server Core e Nano Server não são suportadas, a menos que indicado.
- Para obter detalhes sobre os limites de recursos em uma implantação, consulte Limites.
- Para as versões suportadas do StoreFront, consulte os requisitos de sistema do StoreFront.
- Para obter informações sobre as portas que o Citrix DaaS usa, consulte Portas de Comunicação Usadas pelas Tecnologias Citrix.
- Para obter informações sobre os requisitos ao usar a interface de gerenciamento Quick Deploy, consulte Requisitos.

Limites

Os valores neste artigo indicam os limites de uma única instância do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™). A Citrix testou extensivamente esses limites e os recomenda para a melhor experiência do usuário final e do administrador. Esses limites são limites flexíveis e não são tecnicamente impostos (exceto para o número de domínios do Active Directory e o número total de VDAs por local de recurso). Quando o número de usuários simultâneos excede 125.000, a Citrix pode escalar e combinar várias instâncias do Citrix DaaS para oferecer uma experiência unificada em qualquer escala.

As informações neste artigo são dinâmicas. Verifique frequentemente para atualizações. Se você tiver requisitos atuais que os limites publicados não abordam, entre em contato com seu representante Citrix® para obter assistência o mais cedo possível.

Limites de configuração

Se as políticas excederem o limite, a Citrix recomenda usar o serviço Workspace Environment Management ou Objetos de Política de Grupo do Active Directory (GPOs).

RECURSO	LIMITE
Domínios do Active Directory	250
Pastas de aplicativos	1.000
Grupos de aplicativos	750
Aplicativos	5.000
Catálogos	2.000
Grupos de Entrega	2.000
Conexões de host	200
Locais de recursos	250

RECURSO	LIMITE
Políticas (Studio)	200
Tags	20.000
VDAs	130.000

Limites de local de recurso

A tabela a seguir lista os limites para cada local de recurso.

Se seus requisitos excederem esses limites, a Citrix recomenda usar locais de recurso adicionais.

RECURSO	LIMITE
VDAs totais (limite rígido)	10,000
Sessões totais	25,000
Domínios do Active Directory	1
Conexões de host	40

Os Citrix Cloud Connectors são atribuídos a locais de recurso e vinculam cargas de trabalho ao Citrix DaaS. Para obter informações sobre os limites do Cloud Connector, consulte Considerações sobre tamanho e escala para Cloud Connectors.

Limites de provisionamento

Os limites de provisionamento na tabela a seguir são os máximos recomendados pela Citrix para uma única assinatura de provedor público.

É provável que você atinja os limites de cota do seu fornecedor de nuvem pública em níveis mais baixos. Nesses casos, entre em contato com o fornecedor para aumentar sua cota de assinatura. Para implantações em larga escala, a Citrix recomenda um modelo hub-and-spoke, onde os VDAs são distribuídos por várias assinaturas e conexões de host.

Para obter mais informações, consulte as seguintes arquiteturas de referência:

- Citrix DaaS no AWS

- Virtualização Citrix no Google Cloud
- Citrix DaaS no Azure

RECURSO	LIMITE
VDAs por região AWS	3.000
VDAs por projeto do Google Cloud Platform	3.000
VDA por assinatura do Microsoft Azure por região	5.000

> **Nota:**
>
> Os limites são recomendados pela Citrix.

Limites de uso

Para obter informações sobre as funções de administrador e as diferenças entre elas, consulte:

- Administradores do Manage Studio
- Administradores do Monitor (Director)

RECURSO	LIMITE
Administradores completos simultâneos do Monitor (Director)	40
Administradores de help desk simultâneos do Monitor (Director)	200
Administradores de sessão simultâneos do Monitor (Director)	50
Administradores de nuvem simultâneos do Manage (Studio)	100
Administradores de help desk simultâneos do Manage (Studio)	60

RECURSO	LIMITE
Usuários finais simultâneos	125.000
Recursos publicados para um único usuário	250
Lançamentos de sessão por minuto	3.000

- O Monitor (Director) suporta a agregação de até quatro tenants Citrix DaaS™ (spokes) sob um único tenant (hub).
- Um administrador de help desk na instância hub pode monitorar e solucionar problemas de usuários, máquinas, endpoints e transações de todas as instâncias agregadas (hub e spokes) de acordo com a configuração de Administração Delegada na instância específica.
- O número de administradores simultâneos por instância do Citrix DaaS está de acordo com a tabela Limites de Uso.

Registro de alterações de limites

A tabela a seguir rastreia a modificação do limite de configuração:

DATA	RECURSO	DESCRIÇÃO
18 Feb 2025	Limite de configuração de locais de recursos	O limite aumentou de 200 para 250.
18 Feb 2025	Limite de configuração de domínios do Active Directory	O limite aumentou de 100 para 250.
18 Aug 2025	Limite de configuração de Tags	O limite aumentou de 10.000 para 20.000.
24 Feb 2025	Número de Grupos de Aplicativos	O limite aumentou de 250 para 750.
24 Feb 2025	Número de VDAs	O limite aumentou de 100.000 para 130.000.
12 Dec 2024	Locais de recursos	O limite aumentou de 100 para 200.

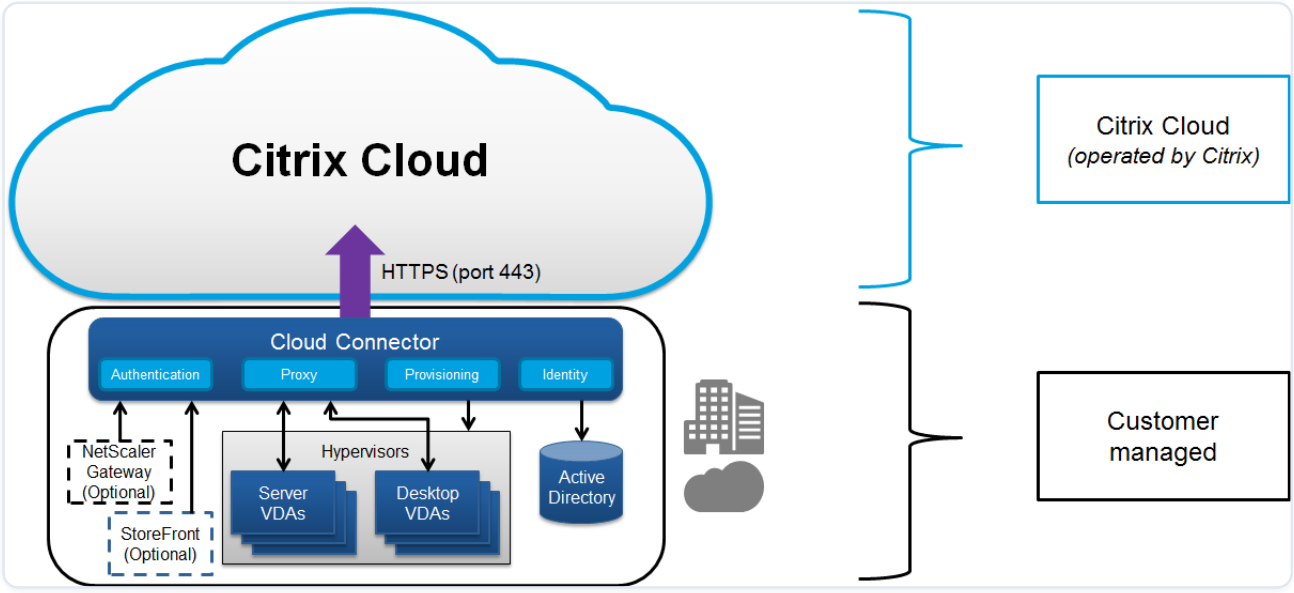
DATA	RECURSO	DESCRIÇÃO
23 May 2024	VDAs por conta AWS por região	O limite aumentou de 1500 para 3000.
22 Nov 2023	Domínios do Active Directory	O limite aumentou de 85 para 100.
	Catálogos	O limite aumentou de 1000 para 2000.
	Grupos de Entrega	O limite aumentou de 1000 para 2000.
	Locais de recursos	O limite aumentou de 85 para 100.
	Localização do recurso -> Sessões totais	Limite aumentado de 20.000 para 25.000.
04 Oct 2023	Tags	O limite aumentou de 500 para 10.000.
07 Dec 2023	Limites de provisionamento -> VDA por assinatura do Microsoft Azure por região	O limite aumentou de 2.500 para 5.000.

Visão geral de segurança técnica

Visão geral de segurança

Este documento se aplica ao Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) hospedado no Citrix Cloud. Esta informação inclui o Citrix Virtual Apps Essentials e o Citrix Virtual Desktops Essentials.

O Citrix Cloud gerencia a operação do plano de controle para ambientes Citrix DaaS. O plano de controle inclui os Delivery Controllers, consoles de gerenciamento, banco de dados SQL, servidor de licenças e, opcionalmente, StoreFront™ e Citrix Gateway. Os Virtual Delivery Agents (VDAs) que hospedam os aplicativos e desktops permanecem sob o controle do cliente no data center de sua escolha, seja na nuvem ou no local. Esses componentes são conectados ao serviço de nuvem usando um agente chamado Citrix Cloud Connector. Se os clientes optarem por usar o Citrix® StoreFront Cloud, eles também podem escolher usar o Citrix Gateway Service em vez de executar o Citrix Gateway em seu data center. O diagrama a seguir ilustra o Citrix DaaS e seus limites de segurança.



Conformidade baseada em nuvem da Citrix

Visite o Citrix Trust Center para obter mais informações sobre as Certificações do Citrix Cloud e verifique frequentemente as atualizações.

Nota:

O uso do Citrix Managed Azure Capacity com várias edições do Citrix DaaS™ e Universal Hybrid Multi-Cloud não foi avaliado para Citrix SOC 2 (Tipo 1 ou 2), ISO 27001, HIPAA ou outros requisitos de conformidade de nuvem.

Fluxo de dados

O Citrix DaaS não hospeda os VDAs, portanto, os dados de aplicativos do cliente e as imagens necessárias para o provisionamento são sempre hospedados na configuração do cliente. O plano de controle tem acesso a metadados, como nomes de usuário, nomes de máquinas e atalhos de aplicativos, restringindo o acesso à Propriedade Intelectual do cliente a partir do plano de controle.

Os dados que fluem entre a nuvem e as instalações do cliente usam conexões TLS seguras pela porta 443.

Isolamento de dados

O Citrix DaaS armazena apenas os metadados necessários para a intermediação e monitoramento dos aplicativos e desktops do cliente. Informações confidenciais, incluindo imagens, perfis de usuário e outros dados de aplicativos, permanecem nas instalações do cliente ou na assinatura de seu provedor de nuvem pública.

Edições do serviço

As capacidades do Citrix DaaS variam por edição. Por exemplo, o Citrix Virtual Apps Essentials™ suporta apenas o serviço Citrix Gateway e o Citrix® StoreFront Cloud. Consulte a documentação do produto para saber mais sobre os recursos suportados.

Segurança ICA®

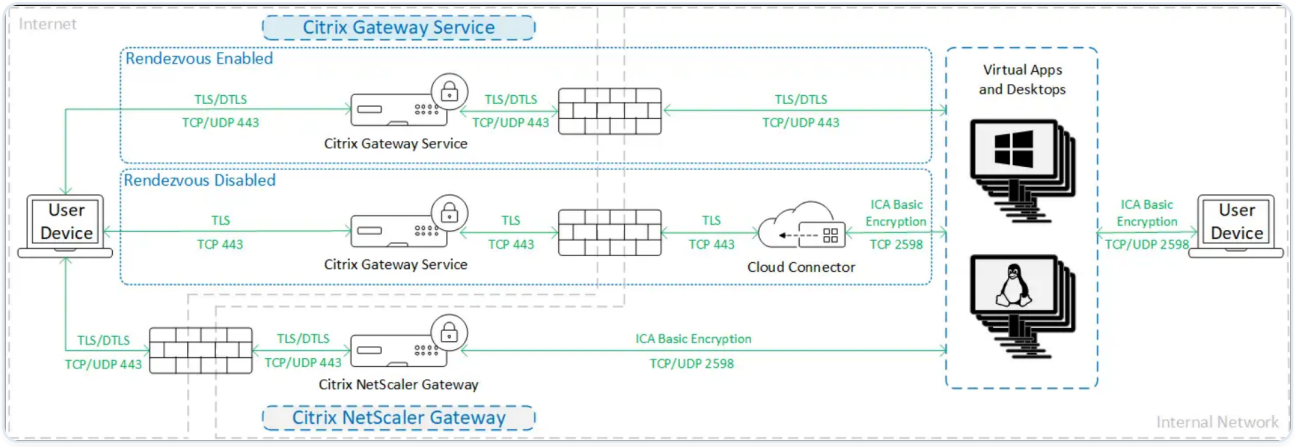
O Citrix DaaS oferece várias opções para proteger o tráfego ICA em trânsito. As opções disponíveis são as seguintes:

- **Criptografia básica:** A configuração padrão.
- **Secure HDX™:** Permite a verdadeira criptografia de ponta a ponta dos dados da sessão usando AES-256.

- **SecureICA:** Permite criptografar dados da sessão usando criptografia RC5 (128 bits).
- **HDX Direct:** Permite usar criptografia em nível de rede usando TLS/DTLS.
- **VDA TLS/DTLS:** Permite usar criptografia em nível de rede usando TLS/DTLS.
- **Protocolo Rendezvous:** Disponível apenas ao usar o Citrix Gateway Service. Ao usar o protocolo Rendezvous, todos os segmentos das conexões das sessões ICA são criptografados usando TLS/DTLS.

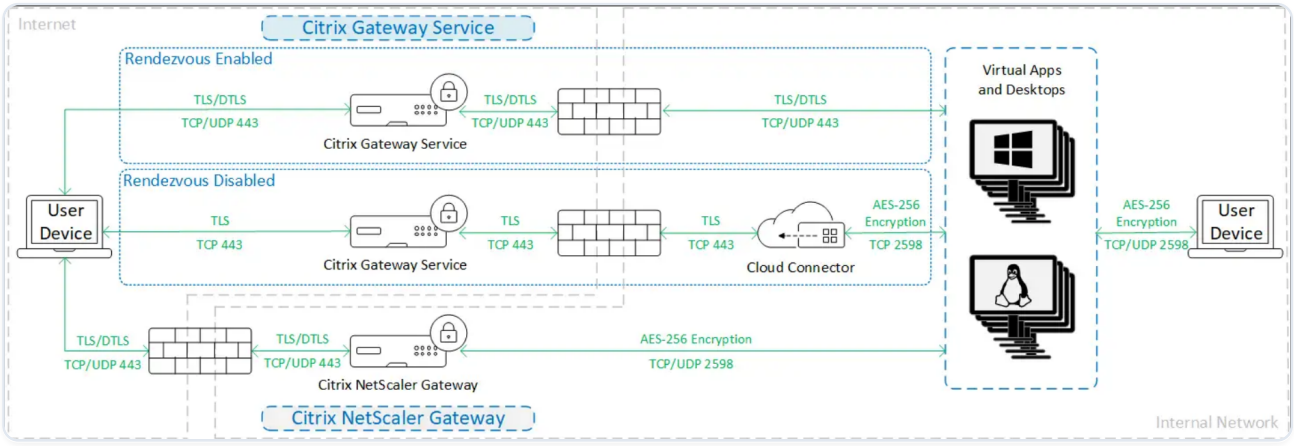
Criptografia básica

Ao usar a criptografia básica, o tráfego é criptografado conforme mostrado no diagrama a seguir.



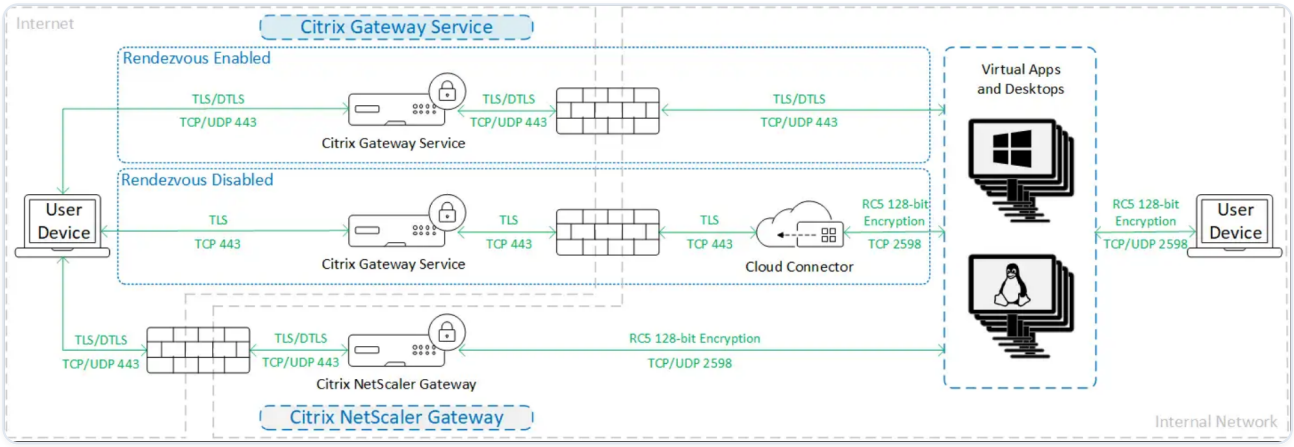
Secure HDX

Ao usar o Secure HDX, o tráfego é criptografado conforme mostrado no diagrama a seguir.



SecureICA

Ao usar o SecureICA, o tráfego é criptografado conforme mostrado no diagrama a seguir.



Nota:

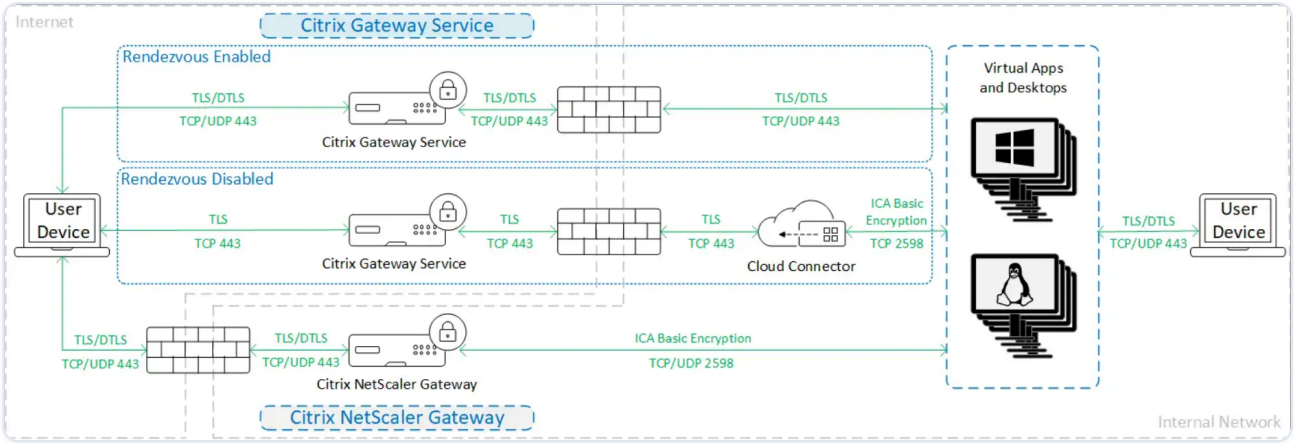
Recomenda-se usar o Secure HDX. O Secure ICA foi descontinuado com o lançamento do Citrix Virtual Apps and Desktops 2402.

O SecureICA não é compatível ao usar o aplicativo Workspace para HTML5.

HDX Direct

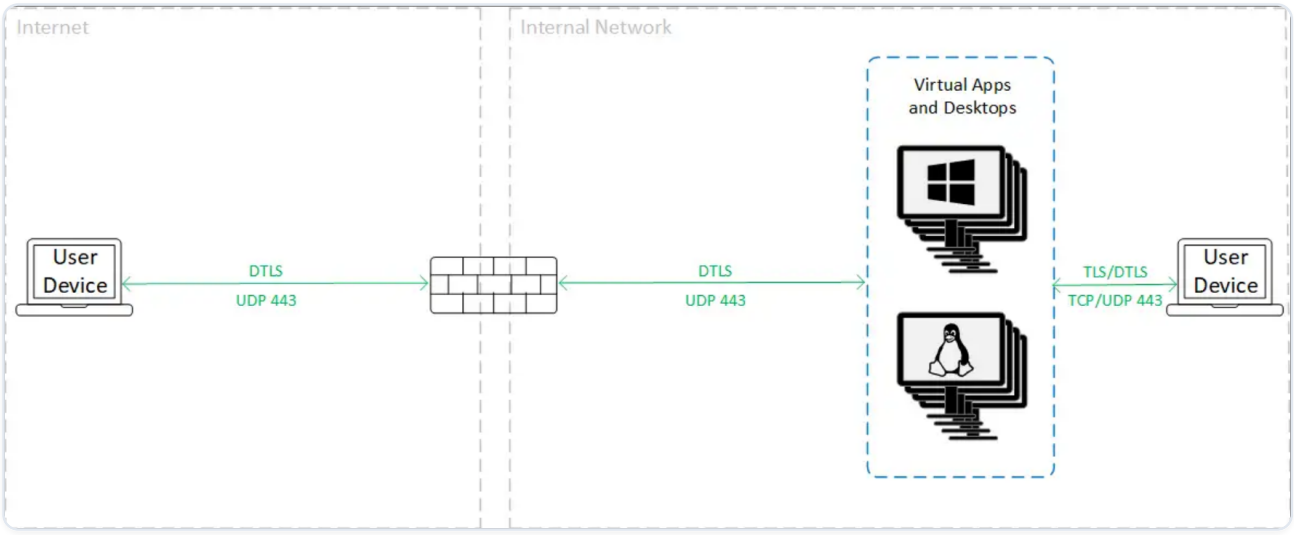
Interno

Ao usar o HDX Direct no modo Somente Interno, o tráfego é criptografado conforme mostrado no diagrama a seguir.



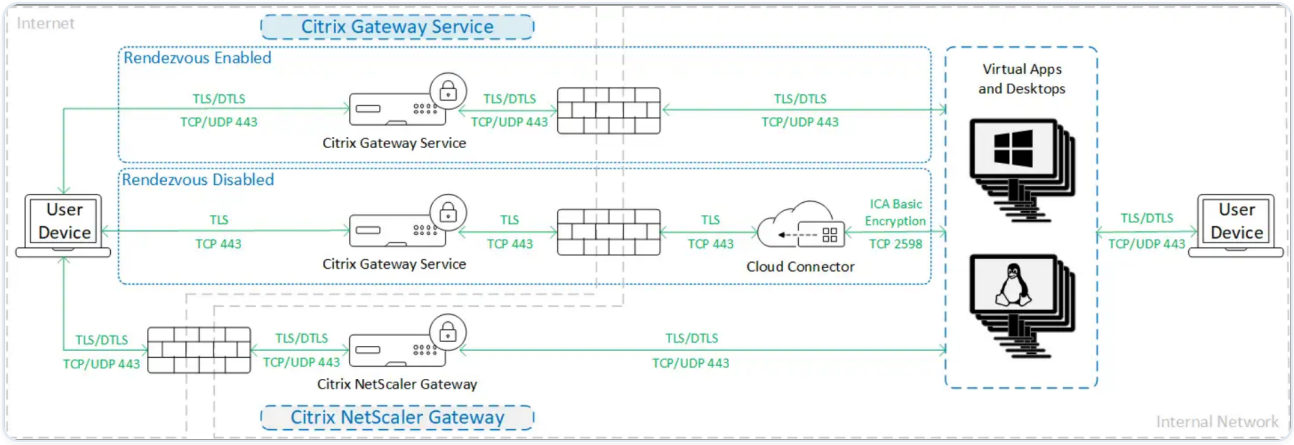
Externo

Ao usar o HDX Direct nos modos Interno e Externo, o tráfego é criptografado conforme mostrado no diagrama a seguir.



VDA TLS/DTLS

Ao usar a criptografia VDA TLS/DTLS, o tráfego é criptografado conforme mostrado no diagrama a seguir.



Nota:

Ao usar o Serviço de Gateway sem Rendezvous, o tráfego entre o VDA e o Cloud Connector não é criptografado por TLS, porque o Cloud Connector não suporta a conexão com o VDA com criptografia em nível de rede.

Mais recursos

Para obter mais informações sobre as opções de segurança do ICA e como configurá-las, consulte:

- HDX Seguro: Secure HDX

- HDX Direto: HDX Direct
- SecureICA: Configurações de política de segurança
- VDA TLS/DTLS: Transport Layer Security
- Protocolo Rendezvous: Rendezvous protocol

Tratamento de credenciais

O Citrix DaaS lida com quatro tipos de credenciais:

- Credenciais de Usuário: Quando os usuários finais autenticar usando seu nome de usuário e senha do Active Directory, estas são armazenadas para fornecer logon único aos VDAs. Ao usar o StoreFront gerenciado pelo cliente, estas são normalmente criptografadas pelo conector antes de serem enviadas ao DaaS; para mais informações, consulte Client access via StoreFront.
- Credenciais de Administrador: Os administradores autenticar contra o Citrix Cloud. A autenticação gera um JSON Web Token (JWT) assinado de uso único que concede ao administrador acesso ao Citrix DaaS.
- Senhas de Hypervisor: Hypervisores locais que exigem uma senha para autenticação possuem uma senha gerada pelo administrador que é armazenada diretamente criptografada no banco de dados SQL na nuvem. A Citrix gerencia chaves de pares para garantir que as credenciais do hypervisor estejam disponíveis apenas para processos autenticados.
- Credenciais do Active Directory (AD): O Machine Creation Services™ usa o Cloud Connector para criar contas de máquina no AD de um cliente. Como a conta de máquina do Cloud Connector tem apenas acesso de leitura ao AD, o administrador é solicitado a fornecer credenciais para cada operação de criação ou exclusão de máquina. Essas credenciais são armazenadas apenas na memória e são mantidas apenas para um único evento de provisionamento.

Considerações de implantação

A Citrix recomenda que os usuários consultem a documentação de melhores práticas publicada para implantar aplicativos Citrix Gateway e VDAs em seus ambientes.

Cloud Connectors

Comunicação com o Citrix Cloud

Todas as conexões dos Citrix Cloud Connectors para DaaS e outros serviços do Citrix Cloud usam HTTPS com TLS 1.2.

HTTPS para serviço XML e STA

Se você usa StoreFront ou NetScaler Gateways locais, é recomendável habilitar HTTPS e desabilitar HTTP no conector. Para obter mais informações, consulte Configuração HTTPS.

Requisitos de acesso à rede

Além das portas descritas em Configuração de portas de entrada e saída, os Cloud Connectors têm os seguintes requisitos de acesso à rede:

- Os Citrix Cloud Connectors exigem apenas tráfego de saída da porta 443 para a internet e podem ser hospedados atrás de um proxy HTTP.
- Dentro da rede interna, o Cloud Connector precisa de acesso ao seguinte para o Citrix DaaS:
  - VDAs: Porta 80, tanto de entrada quanto de saída. mais 1494 e 2598 de entrada se estiver usando o serviço Citrix Gateway
  - Servidores StoreFront: Porta 443 de entrada se estiver usando HTTPS (recomendado) ou porta 80 se estiver usando HTTP (não recomendado).
  - Citrix Gateways, se configurados como um STA: Porta 443 de entrada se estiver usando HTTPS (recomendado) ou porta 80 se estiver usando HTTP (não recomendado).
  - Controladores de domínio do Active Directory
  - Hipervisores: Somente saída. Consulte Portas de comunicação usadas pelas tecnologias Citrix para portas específicas.

O tráfego entre os VDAs e os Cloud Connectors é criptografado usando segurança em nível de mensagem Kerberos.

Chaves de Segurança

Você pode usar Chaves de Segurança para garantir que apenas servidores StoreFront e dispositivos Citrix Gateway autorizados possam se conectar ao DaaS por meio dos conectores de nuvem. Isso é especialmente importante se você tiver habilitado a confiança XML.

Acesso do cliente

Você pode fornecer acesso ao cliente por meio do Citrix® StoreFront Cloud hospedado pela Citrix ou hospedando sua própria implantação do StoreFront.

Os usuários podem se conectar à sua loja usando o aplicativo Citrix Workspace ou um navegador da web. Para recomendações de segurança para o aplicativo Citrix Workspace, consulte a documentação para cada plataforma.

Acesso do cliente via Citrix® StoreFront Cloud

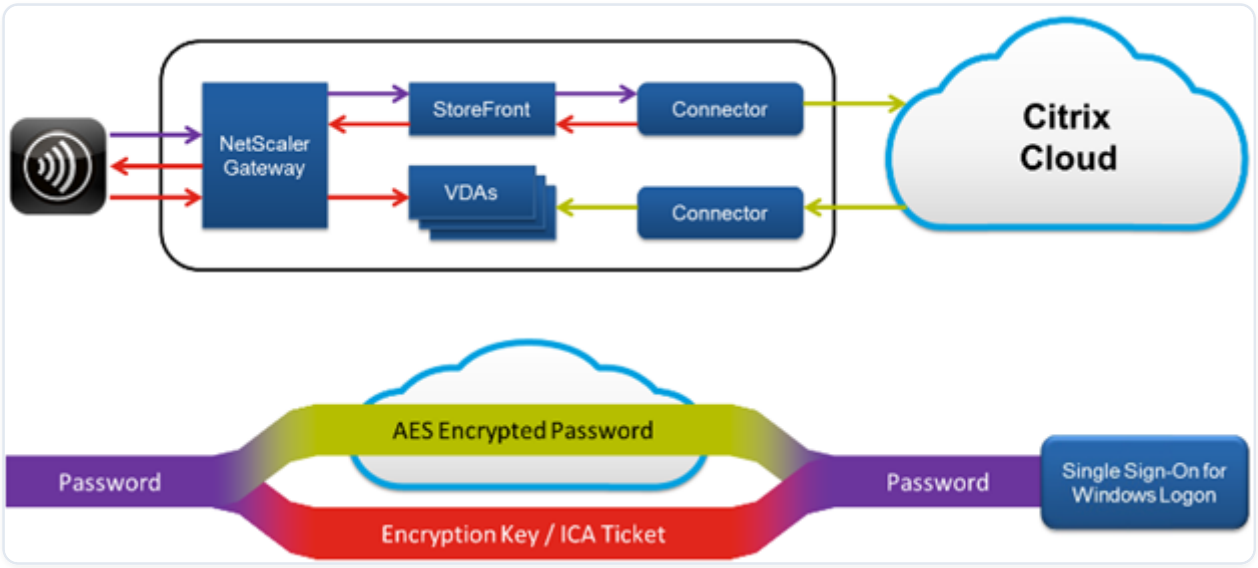
Citrix® StoreFront Cloud é um serviço gerenciado pela Citrix que permite que aplicativos cliente acessem recursos DaaS sem a necessidade de qualquer infraestrutura local. Para versões compatíveis do aplicativo Citrix Workspace e outros requisitos, consulte Requisitos de sistema do Citrix® StoreFront Cloud. Para obter informações sobre segurança, consulte Visão geral de segurança do Citrix® StoreFront Cloud.

Acesso do cliente via Citrix StoreFront

Como alternativa ao Citrix® StoreFront Cloud, você pode fornecer acesso ao cliente implantando o Citrix® StoreFront em seu ambiente local. Isso oferece maiores opções de configuração de segurança e flexibilidade para a arquitetura de implantação, incluindo a capacidade de manter as credenciais do usuário no local. O servidor StoreFront pode ser hospedado atrás de um Citrix Gateway para fornecer acesso remoto seguro, impor autenticação multifator e adicionar outros recursos de segurança. Para obter mais informações, consulte Proteja sua implantação do StoreFront.

Credenciais do usuário

Se o usuário se autenticou no StoreFront com suas credenciais do Active Directory, quando um usuário inicia um aplicativo, o StoreFront passa as credenciais para o Cloud Connector. Por padrão, o Cloud Connector criptografa as credenciais do usuário usando criptografia AES e uma chave aleatória de uso único gerada para cada inicialização. A chave nunca é passada para a nuvem e é retornada apenas para o aplicativo Citrix Workspace. O aplicativo Citrix Workspace então passa essa chave para o VDA para descriptografar a senha do usuário durante o início da sessão para uma experiência de logon único. O fluxo é mostrado na figura a seguir.



É importante que você configure o HTTPS entre o cliente, gateway, StoreFront e conector para garantir que a senha esteja sempre criptografada em sua rede.

Com o comportamento padrão, como o Citrix Cloud não tem acesso às credenciais, ele não consegue encaminhá-las para outros Cloud Connectors ou Connector Appliances para validação. Isso é necessário se você usar vários domínios sem relações de confiança. Você pode desabilitar esse comportamento e permitir que as credenciais sejam carregadas para o Citrix Cloud para que ele possa encaminhá-las para outros Cloud Connectors e Connector Appliances para validação. Para configurar isso, use o cmdlet do SDK do DaaS PowerShell Set-Brokersite com o parâmetro `CredentialForwardingToCloudAllowed`.

Conectando-se aos Cloud Connectors usando HTTPS

Recomenda-se que você configure o StoreFront para se conectar aos Cloud Connectors usando HTTPS para garantir que toda a comunicação seja criptografada. Isso exige que você tenha habilitado HTTPS para serviço XML e STA. Para configurar o StoreFront para se conectar usando HTTPS, consulte Adicionar feeds de recursos para Citrix Desktops as a Service e Adicionar appliance Citrix Gateway.

Confiança XML

Por padrão, quando o StoreFront se conecta ao DaaS para ações como enumeração e inicialização, o StoreFront deve passar as credenciais do Active Directory do usuário para que o DaaS possa autenticar o usuário e verificar a associação do usuário ao grupo. No entanto, ao usar outros métodos de autenticação, como pass-through de domínio, smart cards ou SAML, o StoreFront não possui a senha do Active Directory. Nesse caso, você deve habilitar a "Confiança XML". Com a confiança XML habilitada, o DaaS permite que o StoreFront execute ações em nome de um usuário, como enumerar e iniciar aplicativos sem validar a senha do usuário. Antes de

habilitar a confiança XML, use Chaves de segurança ou outro mecanismo, como firewalls ou IPsec, para garantir que apenas servidores StoreFront confiáveis possam se conectar aos Cloud Connectors.

Para habilitar a confiança XML no Studio, vá para **Configurações > Configurações do site** e ative **Habilitar confiança XML**.

Para usar o SDK do Citrix DaaS para verificar o valor atual da confiança XML, execute Get-BrokerSite e inspecione o valor de `TrustRequestsSentToTheXMLServicePort`.

Para usar o SDK do Citrix DaaS para habilitar ou desabilitar a confiança XML, execute Set-BrokerSite com o parâmetro `TrustRequestsSentToTheXMLServicePort`.

Serviço Citrix Gateway

O uso do serviço Citrix Gateway evita a necessidade de implantar o Citrix Gateway nos data centers do cliente.

Para obter detalhes, consulte Serviço Citrix Gateway.

Todas as conexões TLS entre o Cloud Connector e o Citrix Cloud são iniciadas do Cloud Connector para o Citrix Cloud. Nenhuma porta de firewall de entrada é necessária.

Gateway NetScaler® local

Você pode usar um gateway NetScaler local para fornecer acesso aos recursos. O Gateway deve ser capaz de alcançar os Cloud Connectors para resgatar tickets STA. Recomenda-se configurar o gateway para se conectar aos Cloud Connectors usando HTTPS, consulte HTTPS para serviço XML e STA. Se você habilitou Chaves de segurança, então você deve configurar o gateway para incluir as chaves.

Mais informações

Os seguintes recursos contêm informações de segurança:

- Visão geral de segurança técnica para Citrix Managed Azure.
- Citrix Trust Center: O centro de confiança possui documentação sobre padrões e certificações que são importantes para manter um ambiente de TI seguro e compatível.
- Guia de Implantação Segura para a Plataforma Citrix Cloud: Este guia fornece uma visão geral das melhores práticas de segurança ao usar o Citrix Cloud e descreve as informações que o

Citrix Cloud coleta e gerencia. Este guia também contém links para informações abrangentes sobre o Citrix Cloud Connector.

- Requisitos de Sistema e Conectividade.
- Protegendo aplicativos e desktops virtuais Citrix no local.

> **Nota:**
>
> Este documento tem como objetivo fornecer ao leitor uma introdução e uma visão geral da funcionalidade de segurança do Citrix Cloud; e definir a divisão de responsabilidades entre a Citrix e os clientes no que diz respeito à segurança da implantação do Citrix Cloud. Não se destina a servir como um manual de orientação de configuração e administração para o Citrix Cloud ou qualquer um de seus componentes ou serviços.

Visão geral de segurança técnica para Citrix Managed Azure

Consulte Visão geral de segurança técnica para obter mais informações.

Lista de permissões de canal virtual

A lista de permissões de canal virtual é um recurso que permite controlar quais canais virtuais não-Citrix são permitidos em seu ambiente. Por padrão, o recurso de lista de permissões de canal virtual está habilitado. Como resultado, apenas canais virtuais Citrix têm permissão para abrir em sessões do Citrix Virtual Apps and Desktops™. Se houver necessidade de usar canais virtuais personalizados, sejam eles desenvolvidos internamente ou de terceiros, eles precisam ser explicitamente adicionados à lista de permissões.

Configuração

A lista de permissões de canal virtual está habilitada por padrão. Você pode configurar este recurso usando as seguintes configurações na política Citrix:

- **Lista de permissões de canal virtual**: para habilitar ou desabilitar o recurso e adicionar canais virtuais à lista.
- **Limitação de log da lista de permissões de canal virtual**: define o período de limitação para o registro de eventos da lista de permissões de canal virtual.
- **Registro em log da lista de permissões de canal virtual**: define o nível de registro em log para a lista de permissões de canal virtual.

Adicionando canais virtuais à lista de permissões

Para adicionar um canal virtual à lista de permissões, você precisa das seguintes informações:

1. O nome do canal virtual conforme definido no código, que pode ter até sete caracteres. Por exemplo, `CTXCVC1`.
2. Os caminhos para os processos que abrem o canal virtual na máquina VDA. Por exemplo, `C:\Program Files\Application\run.exe`.

Depois de ter as informações necessárias, você deve adicionar o canal virtual à lista de permissões usando a configuração de política da lista de permissões de canal virtual. Para adicionar um canal virtual à lista, insira o nome do canal virtual seguido por uma vírgula e, em seguida, o caminho para o processo que acessa o canal virtual. Se houver vários processos, você pode adicioná-los separando cada processo com vírgulas.

Para processos únicos

Usando os exemplos anteriores, adicione a seguinte entrada à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Para múltiplos processos

Se houver vários processos, adicione a seguinte entrada à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

Usando curingas

O uso de curingas (*) é suportado. Você pode usar curingas quando os nomes de diretórios ou executáveis mudam com base na versão do aplicativo, ou se o componente de terceiros estiver instalado nos perfis dos usuários.

Você pode usar curingas nos seguintes cenários:

- Para substituir o nome completo do diretório. Por exemplo: `C:\Program Files\Application*\run1.exe`
- Para substituir parte do nome do diretório. Por exemplo: `C:\Program Files\Application\v*\run1.exe`
- Para substituir o nome do executável. Por exemplo: `C:\Program Files\Application\v1.2*.exe`

- Para substituir parte do nome do executável. Por exemplo: `C:\Program Files\Application\v1.2\run*.exe`

As seguintes restrições se aplicam:

- O curinga só pode ser usado para substituir um único diretório. Por exemplo, se o executável estiver localizado em `C:\Program Files\Application\v1.2\run1.exe`
  - Permitido: `C:\Program Files\Application*\run1.exe`
  - Não permitido: `C:\Program Files*\run1.exe`
- As entradas devem conter a extensão do nome do arquivo.
  - Permitido: `C:\Program Files\Application\v1.2*.exe`
  - Não permitido: `C:\Program Files\Application\v1.2*`
- Todos os caminhos devem ser locais.

Nota:

- Caminhos de rede não são permitidos.
- O suporte a curingas está disponível a partir do Citrix Virtual Apps and Desktops 2206.
- O suporte a curingas está disponível no Citrix Virtual Apps and Desktops 2203 LTSR a partir do CU2.

Usando variáveis de ambiente do sistema

Você pode usar variáveis de ambiente do sistema para simplificar a definição dos processos confiáveis em sua lista de permissões. Você pode usar qualquer uma das variáveis prontas para uso, como `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` e `%systemroot%`.

Você também pode usar variáveis de ambiente personalizadas, desde que sejam definidas no nível do sistema.

Os exemplos a seguir descrevem variáveis de ambiente prontas para uso:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

O exemplo a seguir descreve uma variável de ambiente de sistema personalizada:

- Nome da variável personalizada: `app`
- Valor da variável personalizada: `%programfiles%\Application\`
- Entrada da lista de permissões: `CTXCVC1,%app%\run.exe`

> **Observação:**

> Variáveis de ambiente de usuário não são suportadas.

> O suporte a variáveis de ambiente está disponível a partir do Citrix Virtual Apps and Desktops versão 2209.

Obter nomes e processos de canais virtuais

A maneira mais fácil de obter o nome do canal virtual e o processo que o abre na máquina VDA é obter as informações do desenvolvedor ou de um fornecedor terceirizado que forneceu o canal virtual.

Alternativamente, você pode obter informações aplicando os logs do recurso e seguindo estas etapas:

1. Depois que os componentes cliente e servidor do canal virtual personalizado estiverem instalados, inicie um aplicativo virtual ou desktop virtual.
2. No log de eventos do sistema da máquina VDA, procure o nome do canal virtual personalizado e o processo que tentou abri-lo. Para obter mais informações sobre os eventos disponíveis, consulte Logs de eventos.
3. Faça logoff da sessão.
4. Adicione uma entrada nas configurações da política da lista de permissões de canais virtuais para o canal virtual e processo identificados.
5. Reinicie a máquina.
6. Depois que o VDA for registrado, execute o aplicativo virtual ou desktop virtual para validar se os canais virtuais personalizados são abertos com sucesso.

Considerações para canais virtuais Citrix

Todos os canais virtuais Citrix integrados são confiáveis e podem ser abertos sem configuração adicional. No entanto, os dois recursos a seguir exigem entradas explícitas na lista de permissões devido a dependências externas:

- Redirecionamento Multimídia
- HDX RealTime Optimization Pack para Skype for Business

Redirecionamento Multimídia

Se você usar um reprodutor de mídia diferente do Windows Media Player como seu reprodutor de mídia do sistema, precisará adicioná-lo à lista de permissões como um processo confiável. As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXMM`
- Processo: Caminho para o reprodutor de mídia usado em sua máquina VDA. Por exemplo, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Entrada da lista de permissões: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack para Skype for Business

As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXRMEP`
- Processo: Caminho para o executável do Skype for Business em sua máquina VDA, que pode variar dependendo da versão do Skype for Business ou se você usou um caminho de instalação personalizado. Por exemplo, `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- Entrada da lista de permissões: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Métodos de entrega

Um único método de entrega provavelmente não consegue atender a todos os seus requisitos.

Você pode considerar vários métodos de entrega de aplicativos. A escolha do método apropriado ajuda a melhorar a escalabilidade, o gerenciamento e a experiência do usuário.

- **Aplicativo instalado:** O aplicativo faz parte da imagem base da área de trabalho. O processo de instalação envolve dll, exe e outros arquivos copiados para a unidade da imagem, além de modificações no registro. Para obter detalhes, consulte Criar catálogos de máquinas.
- **Aplicativo transmitido (Microsoft App-V):** O aplicativo é perfilado e entregue aos desktops pela rede sob demanda. Os arquivos do aplicativo e as configurações de registro são colocados em um contêiner na área de trabalho virtual, isolados do sistema operacional base e uns dos outros. Essa ação ajuda a resolver problemas de compatibilidade. Para obter detalhes, consulte App-V.
- **Aplicativo em camadas (Citrix App Layering):** Cada camada contém um único aplicativo, agente ou sistema operacional. Ao integrar uma camada de SO, uma camada de plataforma (por exemplo, VDA) e muitas camadas de aplicativo, um administrador pode facilmente criar novas imagens implantáveis. O uso de camadas simplifica a manutenção contínua, pois um SO, agente e aplicativo existem em uma única camada. Ao atualizar a camada, todas as imagens implantadas que contêm essa camada são atualizadas. Consulte Citrix App Layering.
- **Aplicativo Windows hospedado:** Um aplicativo instalado em um host Citrix Virtual Apps multiusuário e implantado como um aplicativo e não como uma área de trabalho. Um usuário acessa o aplicativo Windows hospedado de forma transparente a partir da área de trabalho VDI ou dispositivo de endpoint, ocultando o fato de que o aplicativo está sendo executado remotamente. Para obter detalhes, consulte Criar grupos de entrega.
- **Aplicativo local:** Um aplicativo implantado no dispositivo de endpoint. A interface do aplicativo aparece dentro da sessão VDI hospedada do usuário, mesmo que seja executado no endpoint. Para obter detalhes, consulte Acesso a aplicativos locais e redirecionamento de URL.

Para desktops, você pode considerar desktops publicados do Citrix Virtual Apps™ ou desktops VDI.

Aplicativos e desktops publicados do Citrix Virtual Apps

Use máquinas de SO multi-sessão para entregar aplicativos publicados e desktops publicados do Citrix Virtual Apps.

Caso de uso:

- Você deseja uma entrega baseada em servidor de baixo custo para minimizar o custo de entrega de aplicativos a muitos usuários, ao mesmo tempo em que oferece uma experiência de usuário segura e de alta definição.
- Seus usuários realizam tarefas bem definidas e não exigem personalização ou acesso offline a aplicativos. Os usuários podem incluir trabalhadores de tarefas, como operadores de call center e trabalhadores de varejo, ou usuários que compartilham estações de trabalho.
- Tipos de aplicativo: qualquer aplicativo.

Benefícios e considerações:

- Solução gerenciável e escalável dentro do seu data center.
- Solução de entrega de aplicativos mais econômica.
- Os aplicativos hospedados são gerenciados centralmente e os usuários não podem modificar o aplicativo, proporcionando uma experiência de usuário consistente, segura e confiável.
- Os usuários devem estar online para acessar seus aplicativos.

Experiência do usuário:

- O usuário solicita um ou mais aplicativos do StoreFront™, do menu Iniciar ou de um URL que você fornece a ele.
- Os aplicativos são entregues virtualmente e exibidos perfeitamente em alta definição nos dispositivos do usuário.
- Dependendo das configurações de perfil, as alterações do usuário são salvas quando a sessão do aplicativo do usuário termina. Caso contrário, as alterações são excluídas.

Processar, hospedar e entregar aplicativos:

- O processamento de aplicativos ocorre nas máquinas de hospedagem, em vez de nos dispositivos do usuário. A máquina de hospedagem pode ser uma máquina física ou virtual.
- Aplicativos e desktops residem em uma máquina de SO multi-sessão.
- As máquinas ficam disponíveis por meio de catálogos de máquinas.

- As máquinas dos catálogos de máquinas são organizadas em grupos de entrega que entregam o mesmo conjunto de aplicativos a grupos de usuários.
- Máquinas de SO multi-sessão suportam grupos de entrega que hospedam desktops ou aplicativos, ou ambos.

Gerenciamento e atribuição de sessão:

- Máquinas de SO multi-sessão executam várias sessões a partir de uma única máquina para entregar múltiplos aplicativos e desktops a múltiplos usuários conectados simultaneamente. Cada usuário requer uma única sessão a partir da qual pode executar todos os seus aplicativos hospedados.

  Por exemplo, um usuário faz logon e solicita um aplicativo. Uma sessão nessa máquina fica indisponível para outros usuários. Um segundo usuário faz logon e solicita um aplicativo que essa máquina hospeda. Uma segunda sessão na mesma máquina agora está indisponível. Se ambos os usuários solicitarem mais aplicativos, nenhuma sessão adicional será necessária porque um usuário pode executar vários aplicativos usando a mesma sessão. Se mais dois usuários fizerem logon e solicitarem desktops, e duas sessões estiverem disponíveis nessa máquina, essa única máquina agora usará quatro sessões para hospedar quatro usuários diferentes.
- Dentro do grupo de entrega ao qual um usuário é atribuído, uma máquina no servidor menos carregado é selecionada. Uma máquina com disponibilidade de sessão é atribuída aleatoriamente para entregar aplicativos a um usuário quando esse usuário faz logon.

Aplicativos hospedados em VM

Use máquinas de SO de sessão única para entregar aplicativos hospedados em VM

Caso de uso:

- Você deseja uma solução de entrega de aplicativos baseada em cliente que seja segura, forneça gerenciamento centralizado e suporte muitos usuários por servidor host. Você deseja fornecer a esses usuários aplicativos que são exibidos perfeitamente em alta definição.
- Seus usuários são internos, contratados externos, colaboradores de terceiros e outros membros provisórios da equipe. Seus usuários não exigem acesso offline a aplicativos hospedados.
- Tipos de aplicativos: Aplicativos que podem não funcionar bem com outros aplicativos ou podem interagir com o sistema operacional, como o Microsoft .NET framework. Esses tipos de aplicativos são ideais para hospedagem em máquinas virtuais.

Benefícios e considerações:

- Aplicativos e desktops na imagem são gerenciados, hospedados e executados com segurança em máquinas dentro do seu data center, fornecendo uma solução de entrega de aplicativos mais econômica.
- Após o logon, os usuários podem ser atribuídos aleatoriamente a uma máquina dentro de um grupo de entrega configurado para hospedar o mesmo aplicativo. Você também pode atribuir estaticamente uma única máquina para entregar um aplicativo a um único usuário cada vez que esse usuário fizer logon. Máquinas atribuídas estaticamente permitem que os usuários instalem e gerenciem seus próprios aplicativos na máquina virtual.
- A execução de múltiplas sessões não é suportada em máquinas de SO de sessão única. Portanto, cada usuário consome uma única máquina dentro de um grupo de entrega ao fazer logon, e os usuários devem estar online para acessar seus aplicativos.
- Este método pode aumentar a quantidade de recursos do servidor para processamento de aplicativos e aumentar a quantidade de armazenamento para os vDisks pessoais dos usuários.

Experiência do usuário:

- A mesma experiência de aplicativo contínua que a hospedagem de aplicativos compartilhados em máquinas de SO multi-sessão.

Processar, hospedar e entregar aplicativos:

- O mesmo que máquinas de SO multi-sessão, exceto que são máquinas de SO virtuais de sessão única.

Gerenciamento e atribuição de sessão:

- Máquinas de SO de sessão única executam uma única sessão de desktop a partir de uma única máquina. Ao acessar apenas aplicativos, um usuário pode usar vários aplicativos (e não está limitado a um único aplicativo). O sistema operacional vê cada aplicativo como uma nova sessão.
- Dentro de um grupo de entrega, os usuários logados podem acessar uma máquina atribuída estaticamente (cada vez que o usuário faz logon na mesma máquina) ou uma máquina atribuída aleatoriamente que é selecionada com base na disponibilidade da sessão.

Desktops VDI

Use máquinas de SO de sessão única para entregar desktops VDI do Citrix Virtual Desktops™.

Os desktops VDI são hospedados em máquinas virtuais e fornecem a cada usuário um sistema operacional de desktop.

Os desktops VDI exigem mais recursos do que os desktops publicados do Citrix Virtual Apps, mas não exigem que os aplicativos instalados neles suportem sistemas operacionais baseados em servidor. Além disso, dependendo do tipo de desktop VDI que você escolher, esses desktops podem ser atribuídos a usuários individuais. Isso permite aos usuários um alto nível de personalização.

Ao criar um catálogo de máquinas para desktops VDI, você cria um destes tipos de desktops:

- **Desktop aleatório não persistente, também conhecido como desktop VDI agrupado:** Cada vez que um usuário faz logon em um desses desktops, esse usuário se conecta a um desktop selecionado de um pool de desktops. Esse pool é baseado em uma única imagem. Todas as alterações no desktop são perdidas quando a máquina é reiniciada.
- **Desktop estático não persistente:** Durante o primeiro logon, um usuário é atribuído a um desktop de um pool de desktops. (Cada máquina no pool é baseada em uma única imagem.) Após o primeiro uso, cada vez que um usuário faz logon para usar um desses desktops, esse usuário se conecta ao mesmo desktop que foi atribuído no primeiro uso. Todas as alterações no desktop são perdidas quando a máquina é reiniciada.
- **Desktop estático persistente:** Ao contrário de outros tipos de desktops VDI, os usuários podem personalizar totalmente esses desktops. Durante o primeiro logon, um usuário é atribuído a um desktop de um pool de desktops. Logons subsequentes desse usuário se conectam ao mesmo desktop que foi atribuído no primeiro uso. As alterações no desktop são retidas quando a máquina é reiniciada.

Acesso Remoto a PC

O Acesso Remoto a PC é um recurso do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™) que permite que as organizações permitam facilmente que seus funcionários acessem recursos corporativos remotamente de forma segura. A plataforma Citrix torna esse acesso seguro possível, dando aos usuários acesso aos seus PCs físicos do escritório. Se os usuários puderem acessar seus PCs do escritório, eles poderão acessar todos os aplicativos, dados e recursos de que precisam para realizar seu trabalho. O Acesso Remoto a PC elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, desktops ou aplicativos virtuais e sua infraestrutura associada.

O Acesso Remoto a PC usa os mesmos componentes do Citrix DaaS™ que fornecem desktops e aplicativos virtuais. Como resultado, os requisitos e o processo de implantação e configuração do Acesso Remoto a PC são os mesmos exigidos para a implantação do Citrix DaaS para a entrega de recursos virtuais. Essa uniformidade proporciona uma experiência administrativa consistente e unificada. Os usuários recebem a melhor experiência de usuário usando o Citrix HDX para entregar sua sessão de PC do escritório.

Para obter mais informações, Acesso Remoto a PC.

Planejar e construir uma implantação

Se você não estiver familiarizado com os componentes, terminologia e objetos usados com o Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops), consulte Citrix DaaS.

Se você estiver migrando de uma implantação do Citrix Virtual Apps and Desktops, consulte Migrar para a nuvem.

> **Importante:**
>
> Para garantir que você receba informações importantes sobre o Citrix Cloud™ e os serviços Citrix aos quais você assina, certifique-se de que pode receber todas as notificações por e-mail.
>
> No canto superior direito do console do Citrix Cloud, expanda o menu à direita dos campos de nome do cliente e OrgID. Selecione **Account Settings**. Na guia **My Profile**, selecione todas as entradas na seção **Email Notifications**.

Como usar este artigo

Para configurar sua implantação do Citrix DaaS™, conclua as tarefas resumidas abaixo. Links são fornecidos para os detalhes de cada tarefa.

Revise todo o processo antes de iniciar a implantação, para que você saiba o que esperar. Este artigo também contém links para outras fontes de informação úteis.

> **Nota:**
>
> Se você planeja usar o fluxo de trabalho Quick Deploy para provisionar máquinas Microsoft Azure, siga as orientações de configuração em Introdução ao Quick Deploy.

Planejar e preparar

Na documentação do Citrix Tech Zone, consulte um guia de prova de conceito passo a passo para este serviço.

Inscrever-se

Inscreva-se para uma conta Citrix e solicite uma demonstração do Citrix DaaS.

Configurar um local de recurso

Um local de recurso contém os recursos necessários para entregar aplicativos e desktops aos usuários. A criação de locais de recurso permite que o DaaS use esses recursos. Para saber mais sobre locais de recurso, consulte Conectar ao Citrix Cloud.

Antes de criar máquinas, você deve conectar um local de recurso ao DaaS:

- Máquinas ingressadas no domínio exigem que você tenha Cloud Connectors instalados no local de recurso. Neste caso, você pode criar:
  - Pool de identidade de identidade de máquina ingressada no Active Directory local
  - Pool de identidade de identidade de máquina ingressada no Microsoft Entra
  - Pool de identidade de identidade de máquina ingressada no Microsoft Entra híbrido

  Para alta disponibilidade, recomendamos que você instale dois Cloud Connectors em cada local de recurso. Consulte Instalação do Cloud Connector.

  Mais informações:

  - O que são locais de recurso e Cloud Connectors?
  - Vídeo sobre a instalação de Cloud Connectors:

- Máquinas não ingressadas no domínio não exigem Cloud Connectors, mas exigem que você tenha o Rendezvous V2 habilitado. O protocolo Rendezvous permite que os VDAs ignorem os Cloud Connectors para se conectar direta e seguramente ao DaaS. Consulte Rendezvous V2. Neste caso, você pode:
  - Pool de identidade de identidade de máquina não ingressada no domínio

Se você estiver usando a interface Quick Deploy para provisionar VMs do Azure, a Citrix criará o local de recurso e os Cloud Connectors para você.

Criar uma conexão com o local do recurso

Depois de adicionar um local de recurso e Cloud Connectors, crie uma conexão com o local do recurso usando o Studio.

Esta etapa não é necessária em nenhum dos seguintes casos:

- Você está criando uma implantação simples de prova de conceito
- Você está usando a interface Quick Deploy para provisionar VMs do Azure.

Mais informações:

- O que são hosts?
- O que são conexões de host?

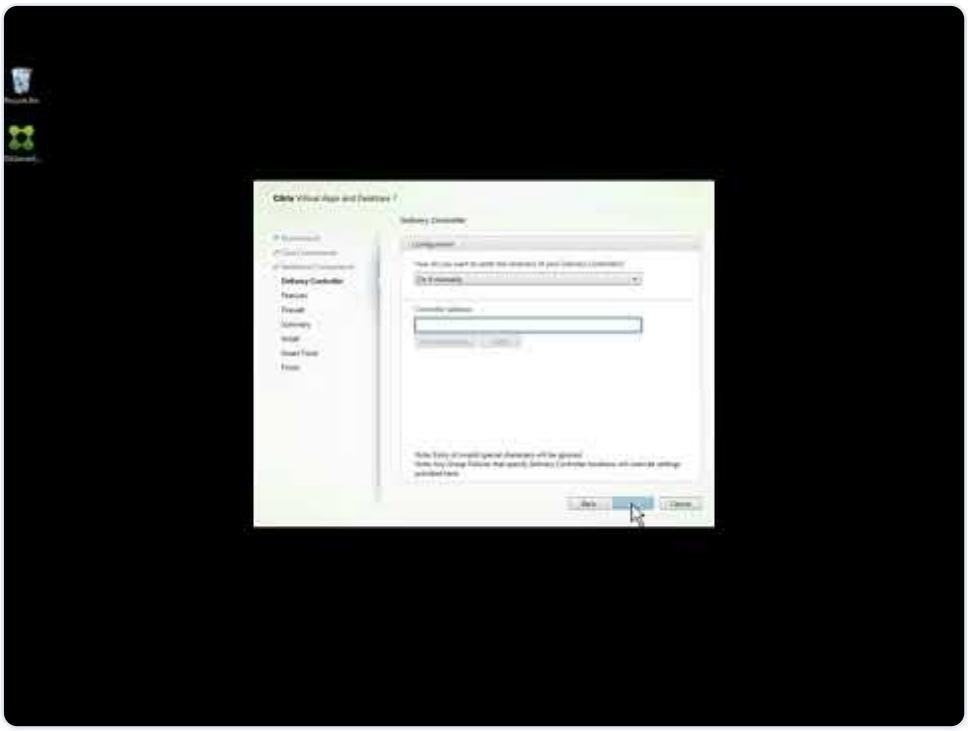
Instalar VDAs

Cada máquina que entrega aplicativos e desktops aos usuários deve ter um Citrix Virtual Delivery Agent (VDA) instalado.

- Para uma implantação simples de prova de conceito, baixe e instale um VDA em uma máquina.
- Se você estiver usando uma imagem para provisionar VMs, instale um VDA na imagem.
- Para uma implantação de Remote PC Access, instale a versão principal do VDA para SO de sessão única em cada PC físico de escritório.

Como fazer e mais informações:

- O que são VDAs?
- Preparação e instrução de instalação
- Instalação do VDA por linha de comando
- Vídeo sobre como baixar e instalar um VDA:

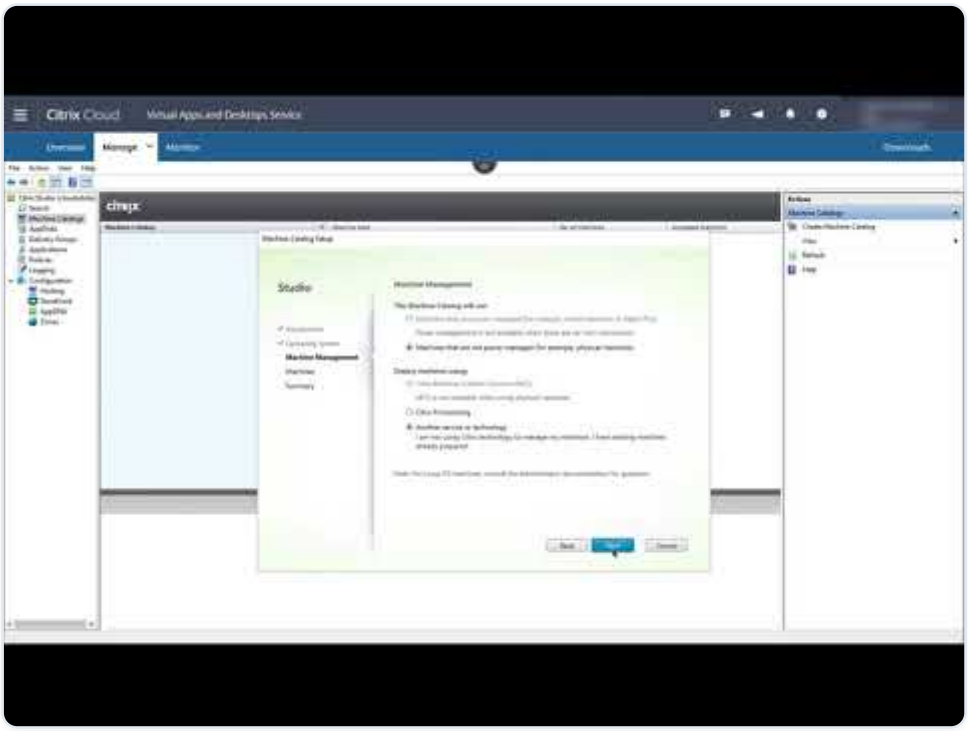


Criar um catálogo

Depois de criar uma conexão com seu local de recurso (se necessário), você cria um catálogo. Se você estiver usando o Studio, o fluxo de trabalho o guiará automaticamente para esta etapa.

Como fazer e mais informações:

- O que são catálogos?
- Criar um catálogo
- Use a interface Quick Deploy para implantar um catálogo contendo VMs do Azure.
- Vídeo sobre como criar um catálogo usando o Studio:



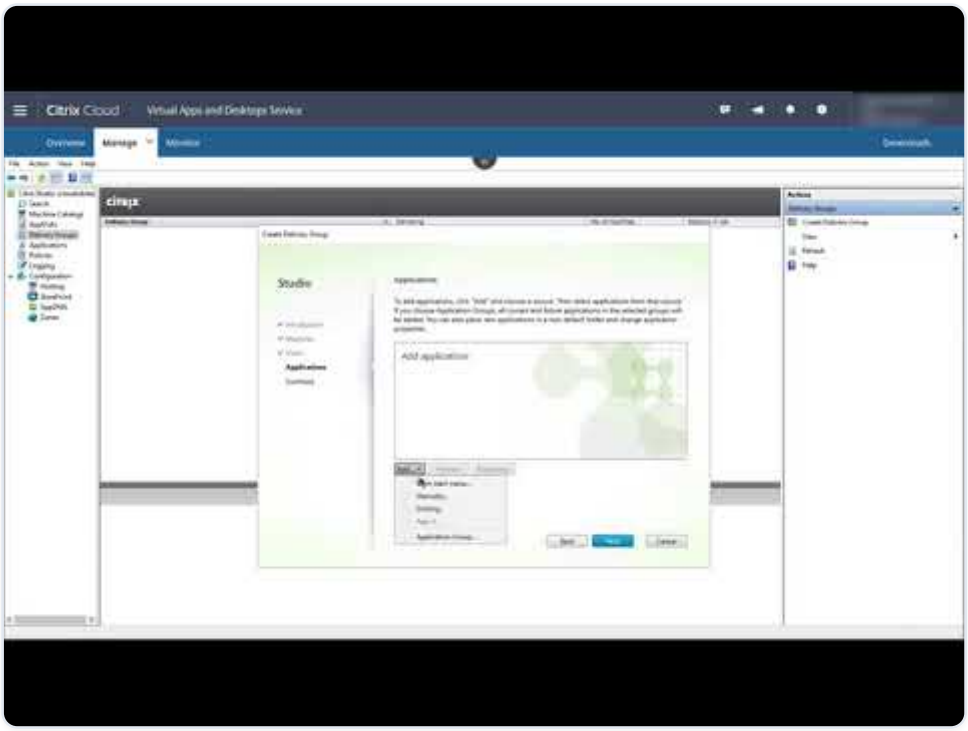
Criar um grupo de entrega

Depois de criar seu primeiro catálogo, o fluxo de trabalho **Gerenciar** o guiará para criar um grupo de entrega.

Esta etapa não é necessária se você estiver usando a interface Quick Deploy para provisionar VMs do Azure.

Como fazer e mais informações:

- O que são grupos de entrega?
- Criar um grupo de entrega
- Vídeo sobre como criar um grupo de entrega:



Implantar outros componentes e tecnologias

Depois de concluir as tarefas acima que configuram a implantação do Citrix DaaS, você encontrará informações sobre o provisionamento e a configuração de outros componentes e tecnologias na solução Citrix, como:

- Políticas Citrix
- StoreFront
- App Layering
- Serviço Workspace Environment Management (WEM)
- Serviço Citrix Gateway
- Zonas
- Serviço de Autenticação Federada (FAS)

Conclua outras tarefas que se aplicam à sua configuração. Por exemplo, se você planeja entregar cargas de trabalho do Windows Server, configure um Servidor de Licenças Microsoft RDS.

Iniciar aplicativos e desktops

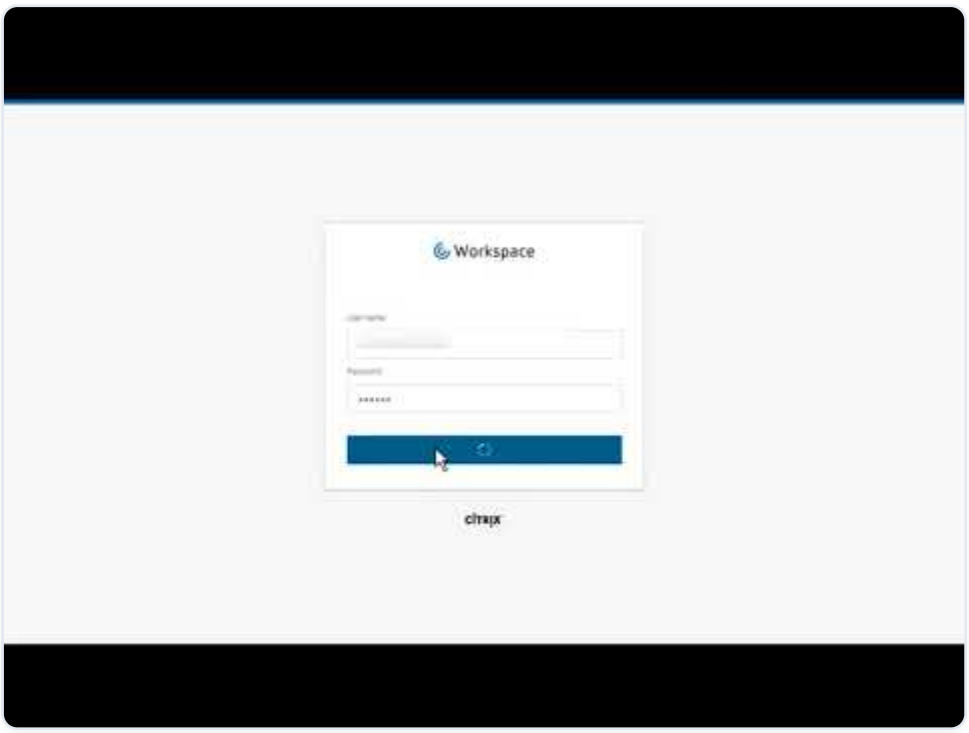
Após configurar sua implantação, a publicação ocorre automaticamente. Os aplicativos e desktops que você configurou ficam disponíveis para os usuários em suas lojas. Um usuário simplesmente navega até o URL de sua loja e seleciona um aplicativo ou desktop, que é iniciado imediatamente.

Envie o URL da loja para seus usuários. Você pode encontrar o URL da loja em dois locais:

- No console do Citrix Cloud, selecione **StoreFront Cloud** no menu no canto superior esquerdo. A guia **Acesso** contém o URL da loja.
- Na página **Visão geral** do Citrix DaaS, o URL da loja aparece perto da parte inferior da página.

Mais informações:

- Vídeo sobre usuários iniciando aplicativos e desktops de suas lojas:



Mais informações

A série de aprendizado do Citrix Cloud oferece cursos educacionais organizados por seu caminho:

- Se você é novo no Citrix DaaS, consulte Caminho de Aprendizado para Novos Usuários do Citrix DaaS.
- Se você está migrando de uma implantação do Citrix Virtual Apps and Desktops, consulte Caminho de Aprendizado para Migração do Citrix Virtual Apps and Desktops para o Citrix Cloud.

Inscrever-se no Citrix DaaS™

Introdução

Você pode assinar o Citrix DaaS através da Citrix ou através do Azure Marketplace.

Se você planeja usar Citrix Managed Azure, também pode solicitar o Fundo de Consumo do Azure da Citrix através da Citrix ou através do Azure Marketplace.

- Ao fazer o pedido através da Citrix, você pode solicitar o Citrix DaaS e o Fundo de Consumo do Azure da Citrix ao mesmo tempo.
- Ao fazer o pedido através do Azure Marketplace, você primeiro solicita o Citrix DaaS. Em seguida, você pode fazer outro pedido para o Fundo de Consumo do Azure da Citrix.

Se você solicitar apenas o Citrix DaaS agora, poderá solicitar o Fundo de Consumo do Azure da Citrix mais tarde, seja através do Azure Marketplace ou do seu representante de conta Citrix.

Demonstrações e avaliações

Você pode avaliar o Citrix DaaS mediante solicitação através da Citrix. A partir de uma avaliação, você pode converter para uma assinatura de serviço paga.

Durante uma avaliação, você pode, opcionalmente, usar uma assinatura do Azure Gerenciado pela Citrix para catálogos, imagens e conexões de rede. Se você tiver recursos gerenciados pela Citrix no momento em que converter para uma assinatura paga, deverá comprar o consumo ou excluir esses recursos gerenciados pela Citrix. Se você não comprar o consumo, esses recursos serão excluídos automaticamente, o que pode afetar os usuários.

Se você assina atualmente um serviço Citrix DaaS

Geralmente, uma conta Citrix Cloud™ permite que você assine apenas um dos serviços do Citrix DaaS (ou uma edição) por vez por Citrix OrgID. Por exemplo, você pode assinar a edição Citrix DaaS Premium OU o Citrix DaaS para Azure, mas não ambos.

Se você assina atualmente um Citrix DaaS e deseja assinar este serviço, você tem duas opções:

- Assine este serviço usando uma conta Citrix Cloud diferente (OrgID).
- Desative o Citrix DaaS que você já possui e, em seguida, solicite este serviço. Para instruções de desativação, consulte CTX239027.

Pedido através da Citrix

Você pode solicitar este serviço (e o Fundo de Consumo do Azure da Citrix) através do Citrix Cloud ou através do seu representante de conta da Citrix.

Através do Citrix Cloud:

- Siga as orientações em Inscrever-se no Citrix Cloud para obter uma conta do Citrix Cloud e um ID de Organização.
- Você pode solicitar uma demonstração do Citrix DaaS. No bloco do Citrix DaaS, clique em **Solicitar Demonstração**. Forneça as informações solicitadas.

  Um representante da Citrix entrará em contato para discutir seus requisitos, ambiente e planos. Dependendo da avaliação do nosso representante, você será autorizado a participar de uma demonstração de administrador ou de um teste de prova de conceito. Para obter mais informações, consulte Testes de Serviço do Citrix Cloud.

Quando você for autorizado para um teste, o texto no bloco do Citrix DaaS no console do Citrix Cloud mudará para **Gerenciar**.

Pedido através do Azure Marketplace

Você pode solicitar as seguintes ofertas da Citrix através do Azure Marketplace:

- Citrix DaaS para Azure
- Citrix DaaS Edição Avançada
- Citrix DaaS Edição Premium
- Workspace Premium Plus

Se você planeja hospedar suas cargas de trabalho do Citrix Virtual Apps and Desktops no Microsoft Azure e deseja usar uma assinatura Azure Gerenciado pela Citrix, solicite o Fundo de Consumo do Azure da Citrix após solicitar o Citrix DaaS ou o Workspace Premium Plus.

Com o Fundo de Consumo do Azure da Citrix, você é cobrado mensalmente pelo seu consumo, que pode variar dependendo dos recursos de hospedagem que você escolher e das horas de uso. Você pode revisar seu uso de consumo através do Citrix Cloud.

Do Azure Marketplace:

- Não é possível combinar o Citrix DaaS e o fundo de consumo em um único pedido.
- O processo de pedido para o Fundo de Consumo do Citrix Azure é essencialmente o mesmo que o pedido do Citrix DaaS, mas você deve ter pedido o Citrix DaaS anteriormente.

Requisitos para fazer pedidos através do Azure Marketplace

- O OrgID da sua conta Citrix Cloud.

  - Se você tem uma conta Citrix Cloud, mas não sabe o OrgID, procure no canto superior direito do console do Citrix Cloud. Ou, verifique o e-mail que você recebeu ao criar a conta.
  - Se você não tem uma conta Citrix Cloud, siga as orientações em Inscrever-se no Citrix Cloud.

- Uma conta Azure e pelo menos uma assinatura Azure nessa conta.

Procedimento para fazer pedidos através do Azure Marketplace

Siga este procedimento para solicitar um Citrix DaaS ou Workspace Premium Plus através do Azure Marketplace. (Se você quiser usar o Citrix Managed Azure, faça outro pedido para o Fundo de Consumo do Citrix Azure, depois de solicitar o Citrix DaaS.)

1. Faça login no Azure Marketplace usando suas credenciais de conta Azure.
2. Pesquise e, em seguida, navegar até a oferta da Citrix que você deseja solicitar.
3. Selecione **Obter agora**.
4. Na mensagem **Mais uma coisa**, preencha as informações necessárias, ative a caixa de seleção de consentimento e, em seguida, selecione **Continuar**.
5. Revise as guias que contêm informações sobre o produto, planos, preços e uso. Quando estiver pronto, selecione um plano (se houver mais de um disponível) e, em seguida, selecione **Configurar + assinar**.
6. Na guia **Básico**:
   - **Assinatura:** Indica o plano que você selecionou.
   - **Grupo de recursos:** Selecione ou crie um grupo de recursos.
   - **Nome:** Insira um nome para o seu pedido de assinatura para que você possa identificá-lo facilmente mais tarde.
   - As informações do **Plano** mostram o preço do plano selecionado, com base no período de faturamento. Para alterar o período do plano, selecione **Alterar plano**. Selecione o período desejado e selecione **Alterar plano**.
7. Na guia **Revisar + assinar**, revise as informações de contato e atualize-as, se necessário. Revise as informações básicas da assinatura. Selecione **Assinar**.
8. Na página **Assinatura em andamento**, selecione **Configurar conta agora**. (Se o botão estiver desativado, aguarde um momento.) Você será levado a uma página de ativação da Citrix.
9. Na página de ativação:

- Use o link **Entrar** para entrar no Citrix Cloud. Um login bem-sucedido preenche automaticamente o campo **ID da Organização**.
- **Quantidade:** Insira o número de usuários. (Um pedido inicial deve ser de pelo menos 25.) Um preço estimado é exibido.
- Concorde com os termos e condições e então selecione **Ativar Pedido**.

Após fazer o pedido via Azure Marketplace

A Citrix envia um e-mail quando seu serviço é provisionado. O provisionamento pode levar algum tempo. Se você não receber o e-mail até o dia seguinte, entre em contato com o Suporte Citrix. Quando você receber o e-mail da Citrix, poderá começar a usar o Citrix DaaS.

O cumprimento de um pedido do Fundo de Consumo do Azure da Citrix não leva muito tempo. Quando a Citrix é notificada do pedido, um banner aparece no console do Citrix DaaS, indicando que uma assinatura do Azure Gerenciado pela Citrix será preparada para você.

Não exclua o recurso Citrix DaaS no Azure. A exclusão desse recurso cancela sua assinatura.

Fazer o pedido pelo Google Cloud Marketplace

Você pode solicitar as seguintes ofertas da Citrix pelo Google Cloud Marketplace:

- Citrix DaaS Standard para Google Cloud
- Citrix DaaS Premium para Google Cloud

Você precisa do seguinte para fazer o pedido pelo Google Cloud Marketplace:

- O OrgID da sua conta Citrix Cloud.
  - Se você tem uma conta Citrix Cloud, mas não sabe o OrgID, procure no canto superior direito do console Citrix Cloud. Ou, verifique o e-mail que você recebeu ao criar a conta.
  - Se você não tem uma conta Citrix Cloud, siga as orientações em Inscrever-se no Citrix Cloud.
- Uma conta Google Cloud e pelo menos uma assinatura Google Cloud nessa conta.

Para fazer seu pedido:

1. Faça login no Google Cloud Marketplace
2. Siga as instruções na página Citrix DaaS para Google Cloud para fazer sua compra.

A Citrix enviará um e-mail quando seu serviço for provisionado. O provisionamento pode demorar um pouco. Se você não receber o e-mail até o dia seguinte, entre em contato com o Suporte Citrix. Ao receber o e-mail da Citrix, você pode começar a usar o Citrix DaaS.

Não exclua o recurso Citrix DaaS no Google Cloud. A exclusão desse recurso cancela sua assinatura.

O que vem a seguir

Depois que seu pedido for atendido, continue com as próximas etapas em Planejar e construir uma implantação.

Por exemplo:

- Se você ainda não configurou seu hipervisor ou serviço de nuvem, ou o Active Directory, consulte Configurar um local de recurso.
- Se seu ambiente de host e o Active Directory já estiverem configurados, consulte Criar uma conexão.

Citrix DaaS™ para Microsoft Azure

Com o Studio, você pode implantar e gerenciar aplicativos e desktops virtuais no Microsoft Azure. As etapas detalhadas são as seguintes:

1. Faça login no Citrix Cloud.
2. Clique no bloco **DaaS** para abrir o Studio.
3. Implante aplicativos e desktops virtuais usando um destes fluxos de trabalho:
    - **Quick Deploy > Microsoft Azure** (recomendado para implantação rápida e guiada). Para obter mais informações, consulte Quick Deploy para Microsoft Azure.

      > **Nota:**
      >
      > Para realizar configurações avançadas ou opções de gerenciamento para sua implantação, use os nós relacionados ao Studio. Para obter mais informações, consulte Studio.

    - **Studio** (recomendado para requisitos de configuração avançada). Para obter mais informações, consulte Introdução: Planejar e criar uma implantação.

Para obter mais informações sobre a diferença entre os fluxos de trabalho Quick Deploy e Studio, consulte a seção a seguir.

Quick Deploy para Microsoft Azure

No Studio, a interface **Quick Deploy > Microsoft Azure** oferece implantação rápida de aplicativos e desktops quando você está usando o Microsoft Azure para hospedar seus desktops e aplicativos. Esta interface oferece configuração *básica*, *sem* recursos avançados.

Com o Quick Deploy, você pode:

- Provisionar máquinas virtuais e catálogos que fornecem desktops e aplicativos hospedados no Microsoft Azure.
- Criar catálogos de Acesso Remoto para PC para máquinas existentes.

Para mais informações, consulte Citrix DaaS Standard for Azure.

> **Nota:**
>
> Com o Quick Deploy, você pode usar uma assinatura Citrix-Managed Azure ou sua própria assinatura do Azure.

Diferenças entre os fluxos de trabalho Quick Deploy e Studio

Como alternativa ao Quick Deploy, o fluxo de trabalho do Studio oferece recursos de configuração avançados. Consulte a tabela a seguir para obter detalhes.

RECURSO	QUICK DEPLOY	STUDIO
Implantar usando o Azure	Sim	Sim *
Imagens preparadas pela Citrix® disponíveis	Sim	Não
Experiência do usuário simplificada	Sim	Não

* Ao usar uma assinatura do Azure gerenciada pela Citrix, você deve usar o Quick Deploy ao criar uma imagem ou catálogo.

Se você está familiarizado com o uso do fluxo de trabalho do Studio para criar e gerenciar catálogos, o Quick Deploy apresenta as seguintes diferenças:

- Terminologia diferente.
  - No Quick Deploy, você cria um catálogo.
  - Em Catálogos de Máquinas, você cria um catálogo de máquinas. Na prática, é frequentemente referido simplesmente como catálogo.
- Localização de recursos e Cloud Connectors.
  - O Quick Deploy cria automaticamente um local de recurso, incluindo dois Cloud Connectors, quando você cria seu primeiro catálogo.
  - No fluxo de trabalho do Studio, criar um local de recurso e adicionar Cloud Connectors são etapas separadas que você deve concluir no Citrix Cloud antes de criar um catálogo.
- Imagens usadas para criar catálogos.
  - O Quick Deploy oferece várias imagens preparadas pela Citrix de máquinas Windows e Linux. Você pode usar essas imagens para criar catálogos.

    Você também pode usar essas imagens para criar imagens e, em seguida, personalizar as novas imagens para atender às suas necessidades exclusivas de implantação. Esse recurso é conhecido como construtor de imagens. Você também pode importar imagens de sua própria assinatura do Azure.
  - No fluxo de trabalho do Studio, você personaliza imagens do host compatível que está usando. As imagens preparadas pela Citrix não estão disponíveis.
- Exibições de catálogo:
  - Catálogos criados no Quick Deploy são visíveis no Quick Deploy e nas exibições da seção Studio.
  - Catálogos criados no fluxo de trabalho do Studio não são visíveis na exibição do Quick Deploy.
- Grupos de entrega:
  - Você não cria grupos de entrega no Quick Deploy. No Quick Deploy, você especifica as máquinas, aplicativos, desktops e usuários (assinantes) no catálogo.

    A Citrix cria automaticamente um grupo de entrega para cada catálogo do Quick Deploy, usando o mesmo nome do catálogo. Essa ação ocorre nos bastidores. Você não precisa

fazer nada para criar o grupo de entrega. O grupo de entrega aparece apenas no nó Grupos de Entrega, não no Quick Deploy.

- No fluxo de trabalho do Studio, você cria um grupo de entrega e indica quais máquinas ele contém. Opcionalmente, você também especifica aplicativos, desktops e usuários. Você também pode criar grupos de aplicativos.

- Layout e interface do usuário.
  - A interface do Quick Deploy tem um layout e estilo diferentes do fluxo de trabalho do Studio. O Quick Deploy contém mais orientações na tela.

As interfaces não são mutuamente exclusivas. Você pode usar o Quick Deploy para criar alguns catálogos e, em seguida, usar o nó Catálogos de Máquinas para criar outros catálogos.

Citrix HDX™ Plus para Windows 365

O Citrix HDX Plus para Windows 365 permite integrar o Citrix Cloud™ com o Windows 365 para usar as tecnologias Citrix HDX para uma experiência de PC na nuvem do Windows 365 aprimorada e mais segura, além de outros serviços do Citrix Cloud para capacidade de gerenciamento aprimorada.

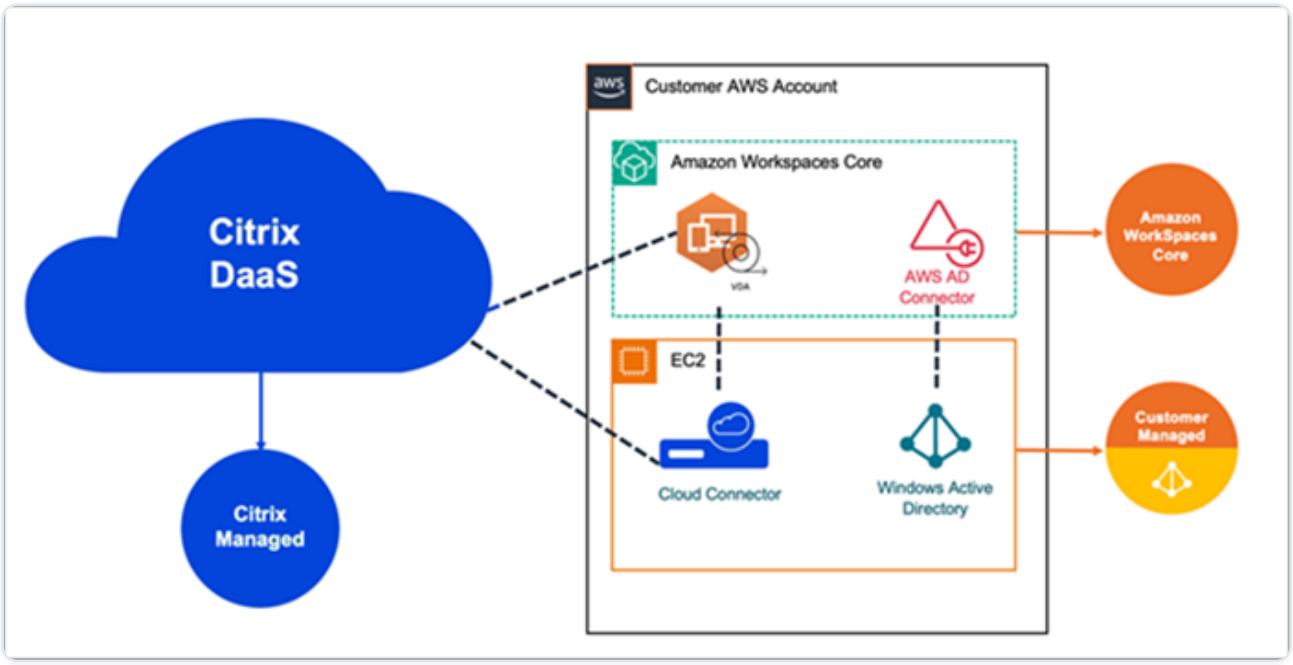
Para obter mais informações, consulte Citrix HDX Plus para Windows 365

Citrix DaaS™ Quick Deploy para Pacotes do Amazon WorkSpaces Core

Introdução

Este artigo descreve como preparar e criar uma implantação com o Citrix® para Amazon WorkSpaces Core. O Amazon WorkSpaces Core reside no Amazon Web Services (AWS).

A seguir está a representação da implementação da AWS e seu gerenciamento com o Citrix DaaS:



Preparar e criar uma implantação

A lista de verificação de implantação na interface **Quick Deploy** contém links para os procedimentos 1-6.

1. Antes de começar, conclua os pré-requisitos no Citrix Cloud e na AWS.
2. Criar um local de recurso no Citrix Cloud. (Este procedimento também está incluído como pré-requisito.)
3. Conectar sua conta AWS. Este procedimento habilita permissões para que o Citrix DaaS possa se conectar à AWS.
4. Criar uma conexão de diretório. Este procedimento configura uma conexão que permite o acesso ao Active Directory da sua organização.
5. Importar uma imagem. Este procedimento permite que você crie uma experiência de desktop para seus usuários.
6. Criar uma implantação. Este procedimento especifica as máquinas a serem implantadas e os usuários que podem acessá-las por meio de sua loja.

Antes de começar

Certifique-se de ter concluído as seguintes tarefas antes de começar a preparar e criar sua implantação.

Há uma exceção: A criação de um local de recurso no Citrix Cloud está listada como um pré-requisito. É também o primeiro procedimento na lista de verificação de implantação. Portanto, se você criar o local de recurso como parte dos pré-requisitos, pule esse procedimento na sequência

da lista de verificação. Da mesma forma, conclua esse procedimento na lista de verificação se você não o fez antes.

Pré-requisitos a serem concluídos no Citrix Cloud

- Crie uma conta Citrix Cloud e assine o Citrix DaaS.
- Crie um local de recurso do Citrix Cloud. (Este procedimento também está vinculado na interface do Quick Deploy.)

Pré-requisitos a serem concluídos na AWS

- Crie uma conta de usuário AWS. A conta deve ter:
  - Permissões de função para o cliente da API Citrix.
  - Permissões para acesso programático. Para obter mais informações, consulte permissões de acesso programático da conta AWS.
  - Crie a função workspaces_DefaultRole. Para obter mais informações, consulte Criar a função workspaces_DefaultRole.
- No seu Active Directory:
  - Use a opção AD Connector para armazenar e gerenciar informações. Para obter mais detalhes, consulte AD Connector.
  - Crie uma OU onde as VMs são criadas. Essa OU deve ter uma política Citrix para comunicação com os Cloud Connectors e o Citrix Cloud. Consulte a seção Referência para obter detalhes.
  - Configure uma política de grupo para a configuração do Citrix Cloud Connector™:
    a. Baixe o Group Policy Management Console mais recente fornecido pela Citrix (CitrixGroupPolicyManagement_64.msi) no site de download da Citrix.
    b. Instale o MSI (essa máquina deve ter o tempo de execução do Visual Studio 2015 instalado). Em seguida, crie uma política Citrix que contenha a configuração da política de Controladores. Essa configuração especifica os endereços do Cloud Connector.
- Crie ou use um gateway NAT existente. Para obter mais informações, consulte gateway NAT.
- Crie ou use um ou mais grupos de segurança existentes que permitam que os Citrix Cloud Connectors se comuniquem com as VMs implantadas. Para obter mais informações, consulte Controlar o tráfego para seus recursos AWS usando grupos de segurança

- Para usar imagens de desktop do Windows 10 ou Windows 11 com tenancy dedicada, configure o BYOL para sua conta. Você pode concluir esta etapa após conectar sua conta. Para obter mais informações, consulte Configurar BYOL para sua conta.

  > **Nota:**
  >
  > As versões Windows 10 N e Windows 11 N não são compatíveis com BYOL.

- Se você planeja usar BYOL, certifique-se de ter licenças suficientes do Windows 10 ou Windows 11. Para obter mais informações, consulte Traga suas próprias licenças de desktop Windows.
- O uso do Citrix DaaS para Amazon WorkSpaces Core habilita automaticamente o recurso Bring Your Own Protocol (BYOP) no Amazon WorkSpaces Core.

Preparação geral

Revise cada procedimento antes de começar. Benefício: Isso ajudará a concluir os processos facilmente.

Criar um local de recurso

Você cria um local de recurso no Citrix Cloud.

- Um local de recurso contém dois ou mais Cloud Connectors que se comunicam com o Citrix Cloud. Os servidores nos quais você instala os Cloud Connectors devem estar em uma VPC EC2, ingressados no domínio e ter conectividade com a Internet. Os Cloud Connectors devem estar na mesma VPC que o diretório que você planeja usar.
- Para obter mais informações sobre Cloud Connectors, consulte Citrix Cloud Connector e como provisioná-los.
- O local de recurso também pode conter seus servidores Active Directory. Para obter mais informações, consulte Conectar o Active Directory ao Citrix Cloud.

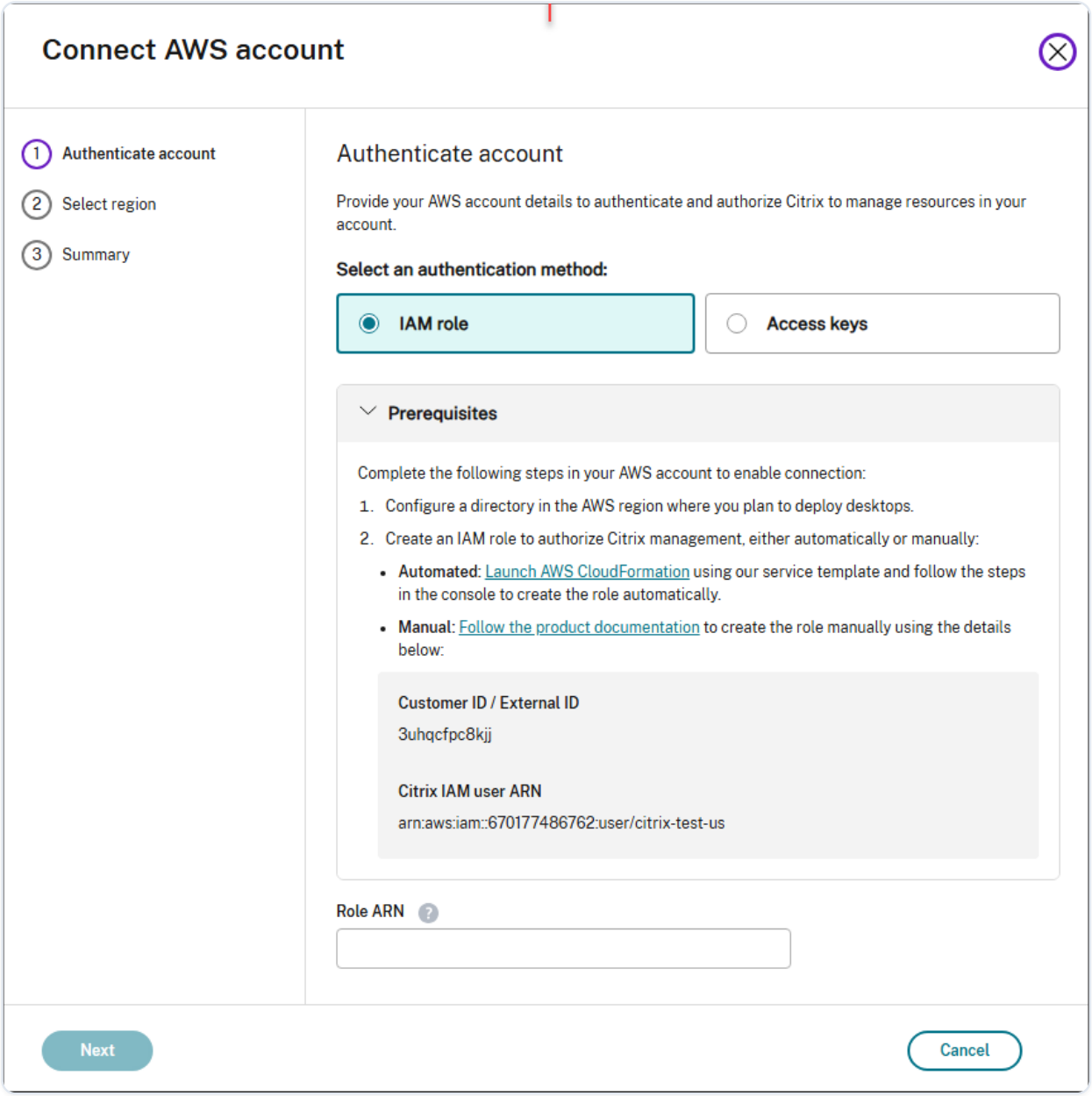
Conecte sua conta AWS

Este procedimento habilita permissões para o Citrix DaaS se conectar ao AWS.

Para conectar sua conta AWS, siga estas etapas:

1. No bloco DaaS, clique em **Gerenciar** para abrir o **Studio**.

2. No painel esquerdo, selecione **Quick Deploy > Amazon WorkSpaces Core > Contas** e, em seguida, clique em **Conectar conta**.



3. Na página **autenticar account**, conclua estas etapas:

   a. Expanda o painel **Pré-requisitos** para revisar os requisitos de configuração.

   b. No painel **Pré-requisitos**, baixe o modelo do AWS CloudFormation do assistente **Conectar conta** e salve-o localmente. Você fará o upload deste modelo mais tarde, ao criar a pilha AssumeRole no AWS.

   c. No campo **ID da Função**, insira o Amazon Resource Name (ARN) da função que autoriza o Citrix a gerenciar seus recursos.

> **Dica:**

- O ID da Função pode ser encontrado no console de gerenciamento da AWS navegando até **IAM > Funções**.
- Se você estiver usando o script `CloudFormation`, então navegar para o CloudFormation e clique na pilha correspondente que foi usada para criar a função. navegar para a guia **Recursos** e clique no recurso com LogicalID `CitrixAssumeRole`.

d. Insira um nome amigável para a conta no campo **Nome**.

e. Clique em **Avançar**. A página **Selecionar região** é aberta.

Nota:

- Você não pode conectar duas contas na mesma região para a mesma conta AWS.
- Para criar um AssumeRole, consulte Criar AssumeRole para integração com Amazon WorkSpaces Core.

4. Na página **Selecionar região**, selecione a região onde você deseja implantar seus desktops e clique em **Avançar**. A página **Resumo** é aberta.
5. Na página **Resumo**, revise as informações fornecidas. Clique em **Conectar**. O processo de conexão pode levar várias horas para ser concluído.

Nota:

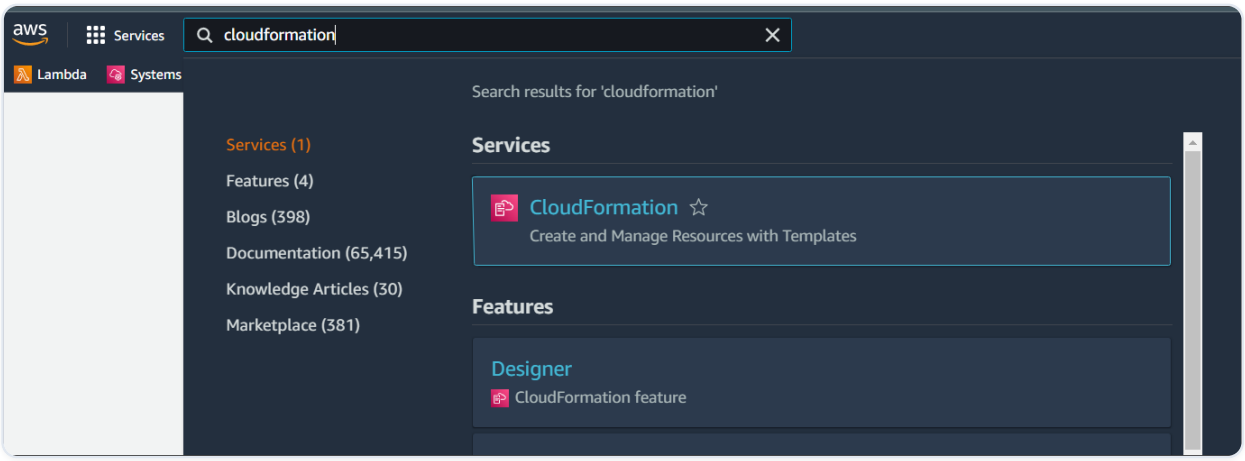
Depois de conectar sua conta, você pode configurar o BYOL a qualquer momento. Para obter mais informações, consulte Configurar BYOL para sua conta.

Criar AssumeRole para integração com Amazon WorkSpaces Core

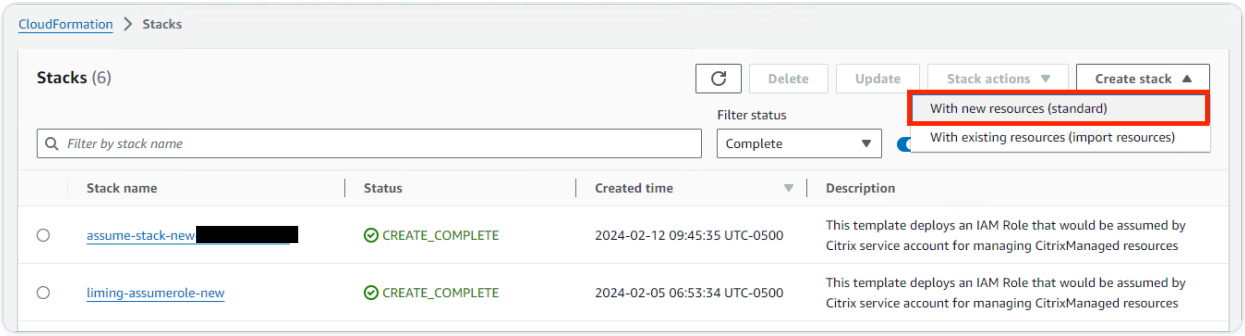
Para criar o AssumeRole para Amazon WorkSpaces Core, siga estas etapas:

1. Na janela do seu navegador, abra o site da **Amazon Web Services** e faça login.

2. No campo **Pesquisar**, digite **cloudformation** e pressione **Enter**.



3. Em **Serviços**, selecione **CloudFormation**. A janela **Stacks** é aberta.

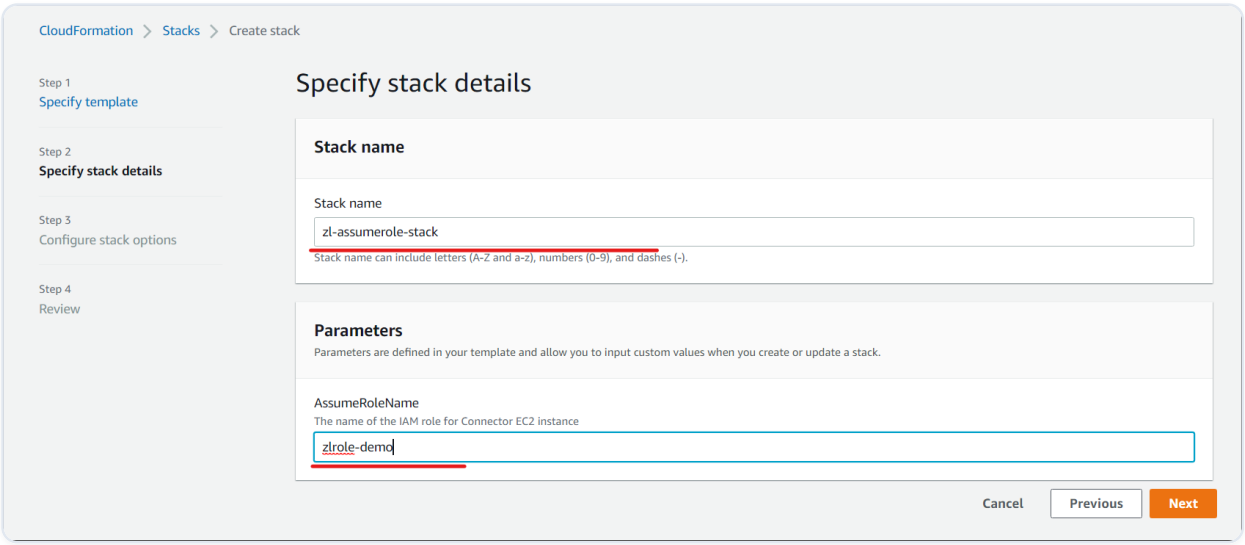


4. Clique em **Criar pilha > Com novos recursos (padrão)** no canto superior direito. A janela **Criar pilha** é aberta.

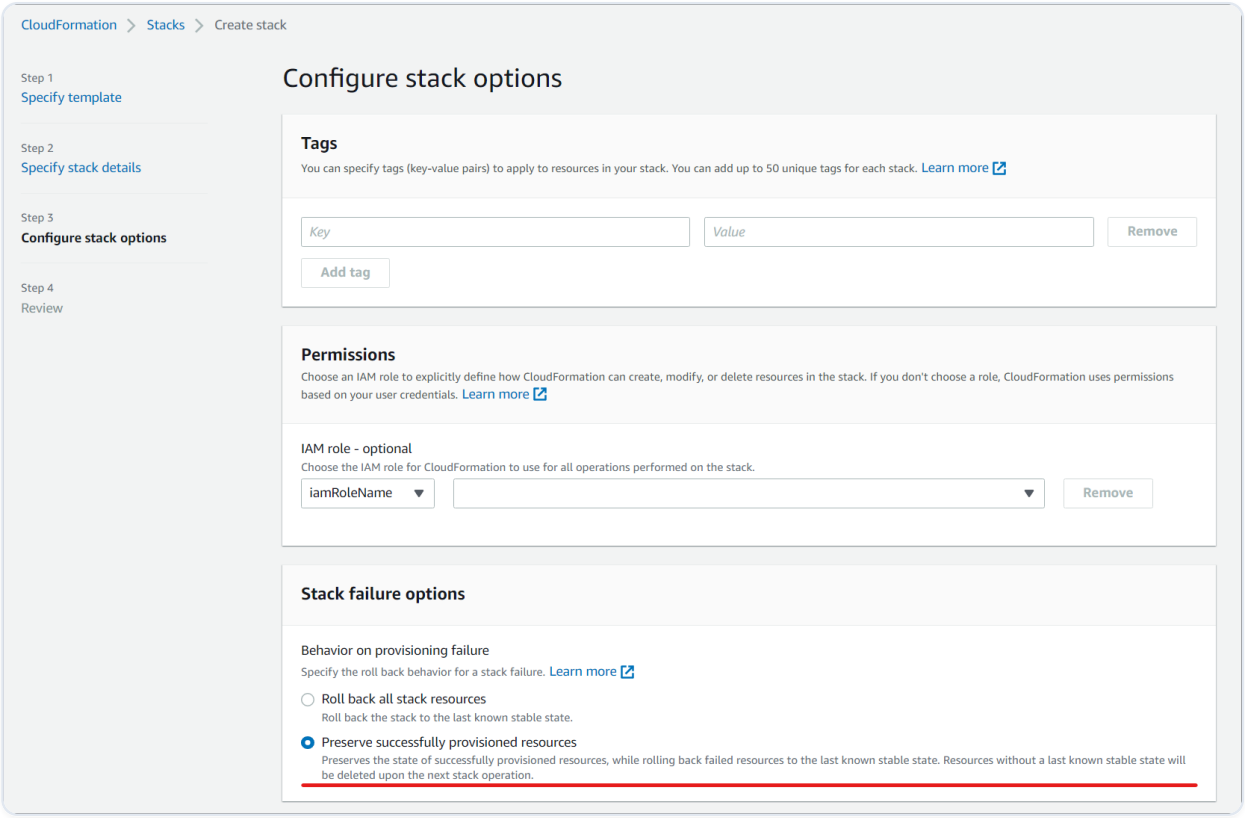
   a. Em **Pré-requisito – Preparar modelo**, selecione **O modelo está pronto**.

   b. Em **Especificar modelo**, clique em **Carregar um arquivo de modelo > Escolher arquivo** e clique em **Avançar**. O painel **Especificar detalhes da pilha** é aberto.

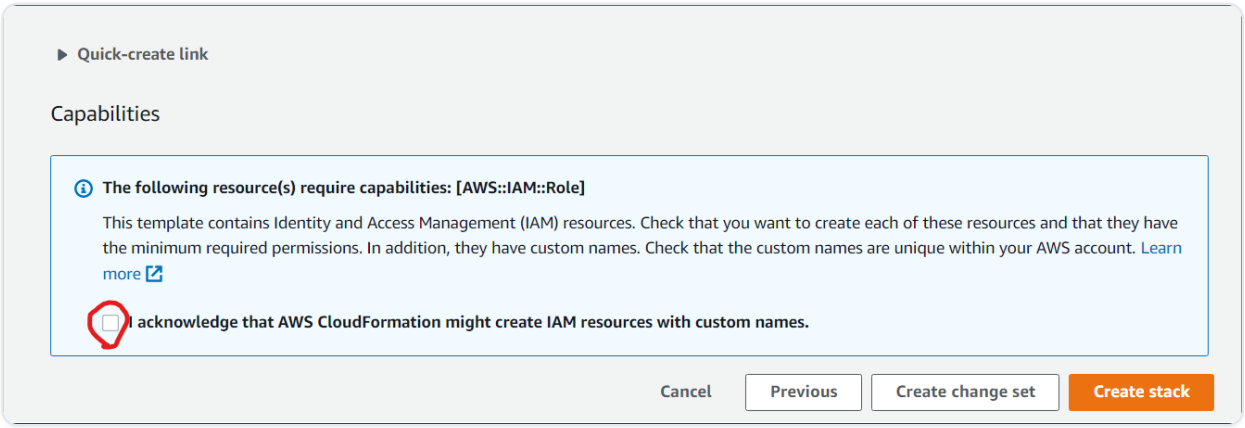
5. No painel **Especificar detalhes da pilha**, forneça um **Nome da pilha** e **AssumeRoleName** e clique em **Avançar**. O painel **Configurar opções da pilha** é aberto.



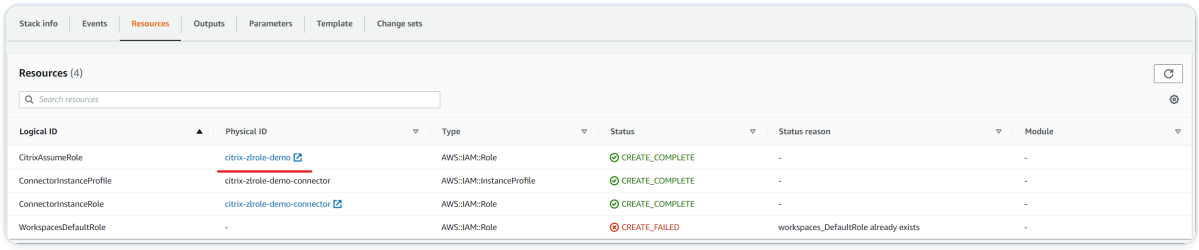
6. No painel **Configurar opções de pilha**, selecione a opção **Preservar recursos provisionados com sucesso**. Esta opção preserva o estado dos recursos provisionados com sucesso. Recursos sem um último estado estável conhecido são excluídos na próxima operação de pilha.



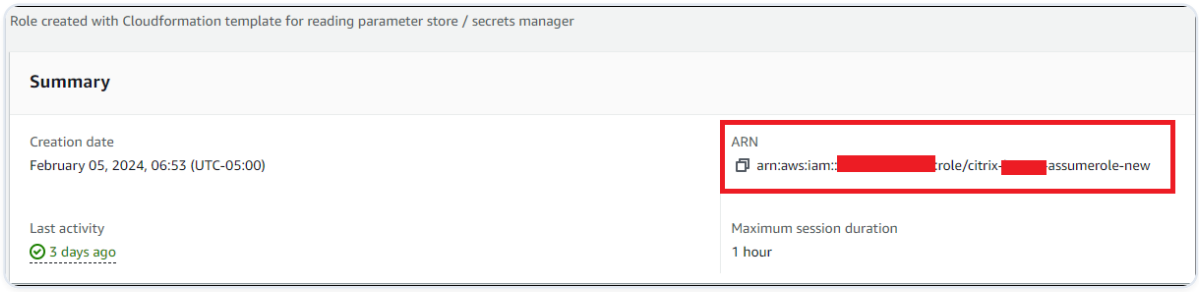
7. Na janela pop-up **Recursos**, selecione a caixa de seleção **Reconheço que o AWS CloudFormation pode criar recursos IAM com nomes personalizados** e clique em **Criar pilha**.



- A guia **Eventos** mostra o status da Pilha criada.
- Na guia **Recursos**, selecione o ID Físico correspondente ao **AssumeRole** criado.



- O painel Resumo mostra o **Nome do Recurso Amazon** (ARN) gerado.



> **Nota:**
>
> A criação da pilha pode falhar porque **workspaces_DefaultRole** já foi criado. Isso não afeta a criação do **AssumeRole**.

8. Retome o procedimento a partir da etapa 3 em Conectar sua conta AWS.

(Opcional) Configure o BYOL para sua conta

Bring Your Own License (BYOL) permite importar e usar imagens de desktop do Windows 10 ou Windows 11 para sua implantação do Citrix DaaS para Amazon WorkSpaces Core. O BYOL permite a tenancy dedicada para conexões de diretório e acesso a imagens de máquina baseadas em EC2.

> **Importante:**
>
> Habilitar o BYOL é uma alteração permanente para sua conta AWS e só pode ser revertida removendo todos os recursos e entrando em contato com o suporte da AWS.

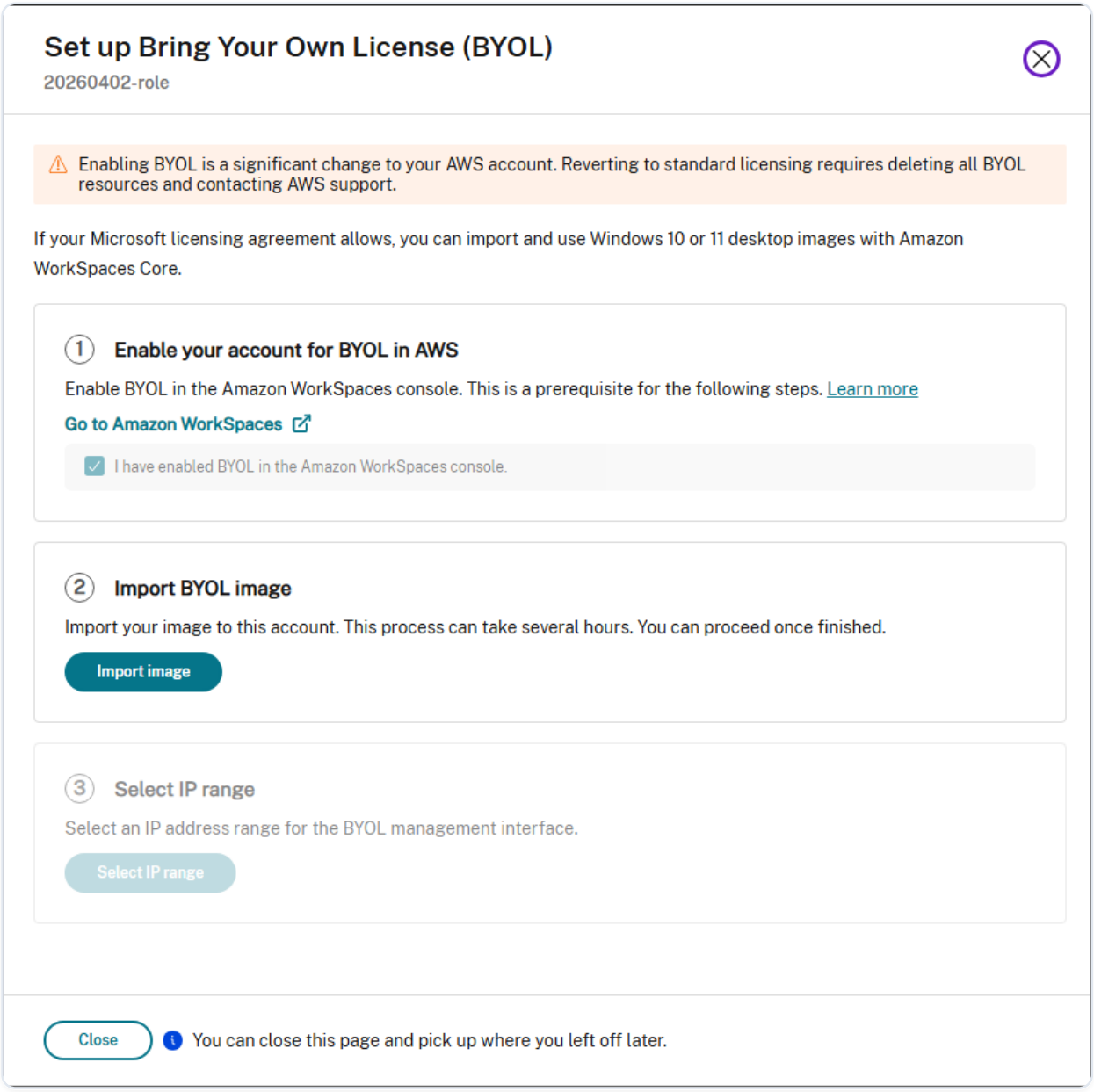
> Você pode configurar o BYOL para uma conta AWS autenticada a partir da lista de **Contas** ou do painel de detalhes da conta.

Pré-requisitos:

- A conta AWS está no estado **Autenticado**.
- O BYOL ainda não foi configurado para a conta.
- O BYOL está habilitado no Console do AWS WorkSpaces para sua conta. Para habilitá-lo, entre em contato com o gerente de contas da AWS, representante de vendas ou o Centro de Suporte da AWS. Para obter mais informações, consulte Habilitar BYOL para sua conta usando o console do Amazon WorkSpaces.

Para configurar o BYOL para sua conta, siga estas etapas:

1. No **Web Studio**, vá para **Quick Deploy > Amazon WorkSpaces Core > Contas**.
2. Selecione a conta AWS para a qual você deseja configurar o BYOL.
3. Clique em **Configurar BYOL**. O assistente **Configurar BYOL** é aberto.



4. Na etapa **Habilitar sua conta para BYOL na AWS**:
    a. Clique em **Ir para Amazon WorkSpaces** para abrir o Console do AWS WorkSpaces e habilitar o BYOL para sua conta.
    b. Depois de habilitar o BYOL na AWS, selecione a caixa de seleção **Confirmar que habilitei o BYOL**.
    c. Clique em **Avançar**.
5. Na etapa **Importar imagem BYOL**, clique em **Importar imagem** para importar uma imagem de desktop do Windows 10 ou Windows 11 para sua conta.

> **Nota:**
>
> A importação de uma imagem pode levar várias horas. Você pode fechar esta página e retornar mais tarde para verificar o status da importação.

Após a conclusão da configuração do BYOL, o painel de detalhes da conta mostra o status do BYOL, o intervalo de IP e as imagens disponíveis.

Criar uma conexão de diretório

> **Nota:**
>
> Cancele o registro do seu Diretório AWS no início desta etapa. Depois de criar uma Conexão de Diretório com o Citrix DaaS, o diretório selecionado é registrado para criar Amazon WorkSpaces com o Citrix DaaS.

> Este procedimento cria uma conexão que permite o acesso ao Active Directory da sua organização.

Pré-requisitos:

- Um local de recurso contendo dois Cloud Connectors.
- Um grupo de segurança.
- Uma OU no seu Active Directory.

Para obter detalhes sobre os pré-requisitos, consulte Antes de começar.

Você pode iniciar este procedimento de um de dois lugares:

- Um link na lista de verificação Primeiros passos.
- No Studio, selecione **Studio > Quick Deploy > Amazon WorkSpaces Core > Directory connections**. Em seguida, clique em **Create Directory Connection**.

Siga a sequência **Create directory connection**:

1. **Connect directory:** Selecione a conta no menu suspenso. Selecione **Dedicated** ou **Shared** para a tenancy.
2. **Resource location:** Selecione a conta e o diretório. (A conta selecionada deve ter pelo menos um diretório.)
    - Selecione duas sub-redes nas quais as máquinas de desktop serão implantadas. As sub-redes devem estar em zonas de disponibilidade apropriadas.
    - Especifique um nome amigável para esta conexão.
    - Quando terminar, clique em **Next**.
3. **Virtual machine settings:** As configurações selecionadas se aplicam a todas as VMs que usam esta conexão de diretório.
    - A OU selecionada deve corresponder à OU visada pela Política de Grupo do Citrix.
    - Selecione um grupo de segurança.
    - Indique se deseja conceder privilégios de administrador a cada usuário atribuído às VMs.

Importar uma imagem

Este procedimento permite criar uma experiência de desktop para seus usuários. Agora você pode importar dois tipos de imagens:

- Imagem EC2 - Para importar esta imagem, o pré-requisito é instalar o Citrix Virtual Delivery Agent e todos os seus drivers. A imagem também deve ser preparada para BYOL. Um script BYOL está disponível em: BYOLChecker.zip.
- Imagem do Workspace - Para importar esta imagem, o pré-requisito é instalar o Citrix Virtual Delivery Agent e todos os seus drivers.

Para importar a imagem, siga as etapas:

1. Em **Web Studio > Quick Deploy > Amazon WorkSpaces Core**, clique em **Imagens**.
2. Em **Minhas Imagens**, clique em **Importar Imagem**.

a. **Pré-requisitos:** Fornece os detalhes dos pré-requisitos para a imagem EC2 e a imagem do Workspace. Clique em **Avançar: Escolher imagem**.

b. **Escolher imagem**

- Forneça um nome amigável para a imagem.
- Selecione uma conta.
- Na lista suspensa **Imagem**, você pode selecionar imagens do tipo EC2 ou WSI.
  - Se você selecionar **EC2**, escolha o aplicativo a ser instalado no menu suspenso **Aplicativo** e clique em **Avançar: Resumo**. Imagens do tipo EC2 suportam apenas sessões únicas.
  - Se você selecionar **WSI**, certifique-se de que o suporte à sessão e o processo de ingestão estejam alinhados com a configuração da imagem. Embora uma incompatibilidade não sobrescreva as configurações da imagem, ela pode causar falha na implantação devido à incompatibilidade. Selecione o suporte à sessão como sessão única ou multi-sessão.
- Forneça uma descrição e clique em **Avançar: Resumo**.
- Clique em **Avançar**. A página **Resumo** é aberta.

3. Na página **Resumo**, revise as informações fornecidas e clique em **Importar Imagem**.

> **Nota:**
>
> A importação de uma imagem pode levar várias horas.

4. Selecione qualquer imagem e clique em **Ver Detalhes**. A página de detalhes mostra as opções selecionadas ao criar as imagens, como Conta, Suporte à sessão, Locação, Aplicativos e outros.

> **Nota:**
>
> Ao criar uma implantação, na página **Imagem e desempenho**:

- Se a **Conexão de diretório** selecionada tiver uma locação dedicada, as imagens listadas serão apenas de sessão única. Na página **Desktops**, você pode optar por criar desktops com ou sem atribuição de usuários.
- Se a conexão de diretório selecionada tiver uma locação compartilhada, as imagens listadas serão de sessão única e multissessão. Se você selecionar uma imagem com multissessão, na página **Desktops**, apenas a opção **Criar desktops sem atribuir usuários** estará habilitada.

Requisitos para Imagens de Locação Dedicada

- As imagens devem ser Windows 10 Pro ou Windows 11 Pro.
- Execute o script BYOLChecker durante a preparação da imagem.
- A imagem só pode ser configurada para suporte de sessão única.
- Ao criar uma imagem AMI no EC2, o snapshot deve estar descriptografado.
- O protocolo de ingestão padrão durante a importação de imagem é regular. No entanto, os clientes podem optar pelo protocolo de ingestão gráfica G4DN, que instala drivers adicionais e requer máquinas de nível superior.
- Durante a importação da imagem, os clientes podem adicionar um aplicativo de escritório para ser instalado. Isso limitará a criação de workspaces a implantações de usuários pré-atribuídos.
- As imagens exigem que a conexão de diretório seja definida como dedicada.
- Você pode criar implantações de sessão única pré-atribuídas ou implantações de sessão única desacopladas (agrupadas).

Requisitos para Imagens de Locação Padrão ou Compartilhada

- Selecione o pacote BYOP do Windows Server para criar um workspace.
- O workspace deve ser não criptografado, e apenas o modo **Always On** é suportado.
- Conecte-se ao workspace a partir do conector usando o endereço IP privado via RDP e faça login com as mesmas credenciais de usuário às quais o workspace está atribuído. A imagem não pode ser salva se houver vários perfis de usuário na máquina.
- Instale o VDA e execute o aplicativo verificador de imagem.
- O VDA pode ser configurado como sessão única ou multissessão.
- Reinicie o workspace e salve-o como uma imagem.
- Depois que a imagem for salva, ela poderá ser importada para o ambiente Citrix.

- O protocolo de ingestão padrão durante a importação de imagem é regular. No entanto, se o pacote base for baseado em G4DN, você pode optar pelo protocolo de ingestão gráfica G4DN.
- As imagens exigem que a conexão de diretório seja definida como compartilhada.
- Se você configurou e salvou a imagem como sessão única, pode criar implantações de sessão única pré-atribuídas ou implantações de sessão única desacopladas (agrupadas).
- Se você configurou e salvou a imagem como multissessão, só poderá criar implantações de multissessão desacopladas (agrupadas).

Compatibilidade de SO, Tipo de Diretório e Suporte a Sessão

IMAGEM	SUPORTE A SESSÃO	TENANCY DE DIRETÓRIO AWS	TIPO DE IMPLANTAÇÃO	PERSISTÊNCIA
Windows Desktop 11 Pro	Sessão Única	Dedicado	Dedicado ou Agrupado	Persistente
Windows Desktop 10 Pro	Sessão Única	Dedicado	Dedicado ou Agrupado	Persistente
Windows Server 2022	Multi-Sessão	Compartilhado	Agrupado	Persistente
Windows Server 2022	Sessão Única	Compartilhado	Dedicado ou Agrupado	Persistente
Windows Server 2019	Multi-Sessão	Compartilhado	Agrupado	Persistente
Windows Server 2019	Sessão Única	Compartilhado	Dedicado ou Agrupado	Persistente

Nota:

Todas as instâncias são persistentes e, usando o recurso de pools, as instâncias são atribuídas com base no primeiro uso. As instâncias permanecem provisionadas sem um usuário atribuído. Quando um usuário faz login pela primeira vez, essa instância é atribuída ao usuário para todos os logins futuros.

Integrar imagem do Microsoft Office 2019 ao importar uma imagem

Para integrar a imagem do Microsoft Office 2019 ao importar uma imagem:

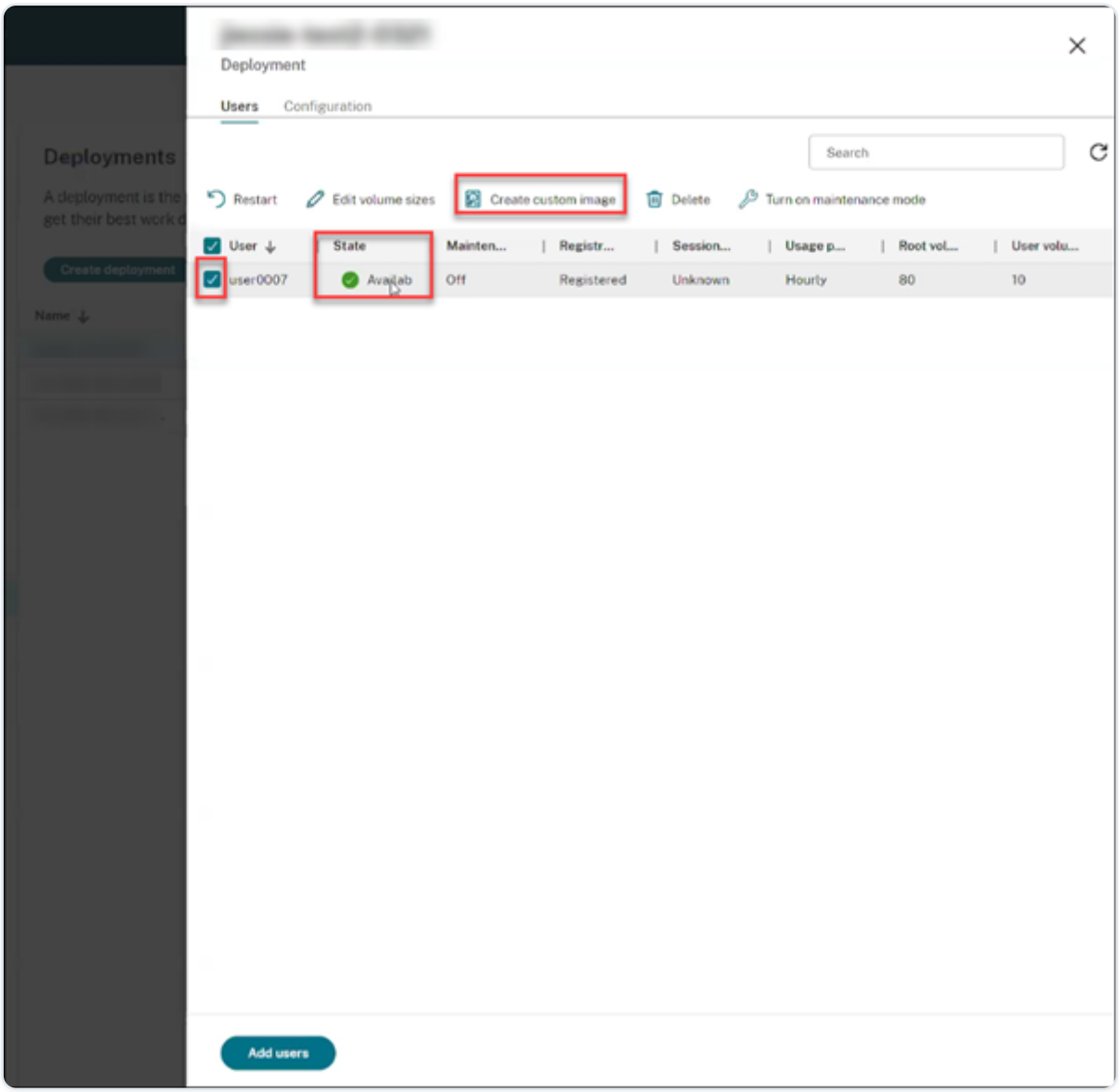
1. Em **Web Studio > Quick Deploy > Amazon WorkSpaces Core**, clique em **Imagens**.
2. Em **Minhas Imagens**, clique em **Importar Imagem**.
3. Em **Importar Imagem > Pré-requisitos**, clique em **Avançar: Escolher Imagem**.
4. Em **Importar Imagem > Escolher imagem:**
    - Selecione uma conta no menu suspenso **Conta**.
    - Selecione uma AMI no menu suspenso **AMI**.
    - Insira o nome da imagem no campo **Nome**.
    - Selecione **Incluir Microsoft Office 2019 Professional Plus** na imagem.
    - Insira uma descrição no campo **Descrição**.
5. Em **Import Image > Choose image**, clique em **Next: Summary**.
6. Em **Choose Image > Summary**, certifique-se de que **Selected** apareça para **Microsoft Office 2019**.
7. Em **My Images**, clique em **Import Image**. O status da imagem implantada recentemente exibe **importing** até que a operação de importação seja concluída.
8. Em **My Images**, selecione a imagem implantada recentemente e clique em **View Detail**.
9. No painel **Detail**, o campo **Microsoft Office 2019** exibe **Included**.

> **Nota:**
>
> Somente as seguintes versões do SO são compatíveis:
>
> - Windows 10 Version 21H2 (December 2021 Update)
> - Windows 10 Version 22H2 (November 2022 Update)
> - Windows 10 Enterprise LTSC 2019 (1809) (1809)
> - Windows 10 Enterprise LTSC 2021 (21H2) (21H2)
> - Windows 11 Versão 22H2 (lançamento de outubro de 2022)

Criar uma imagem personalizada a partir de uma instância WorkSpaces existente

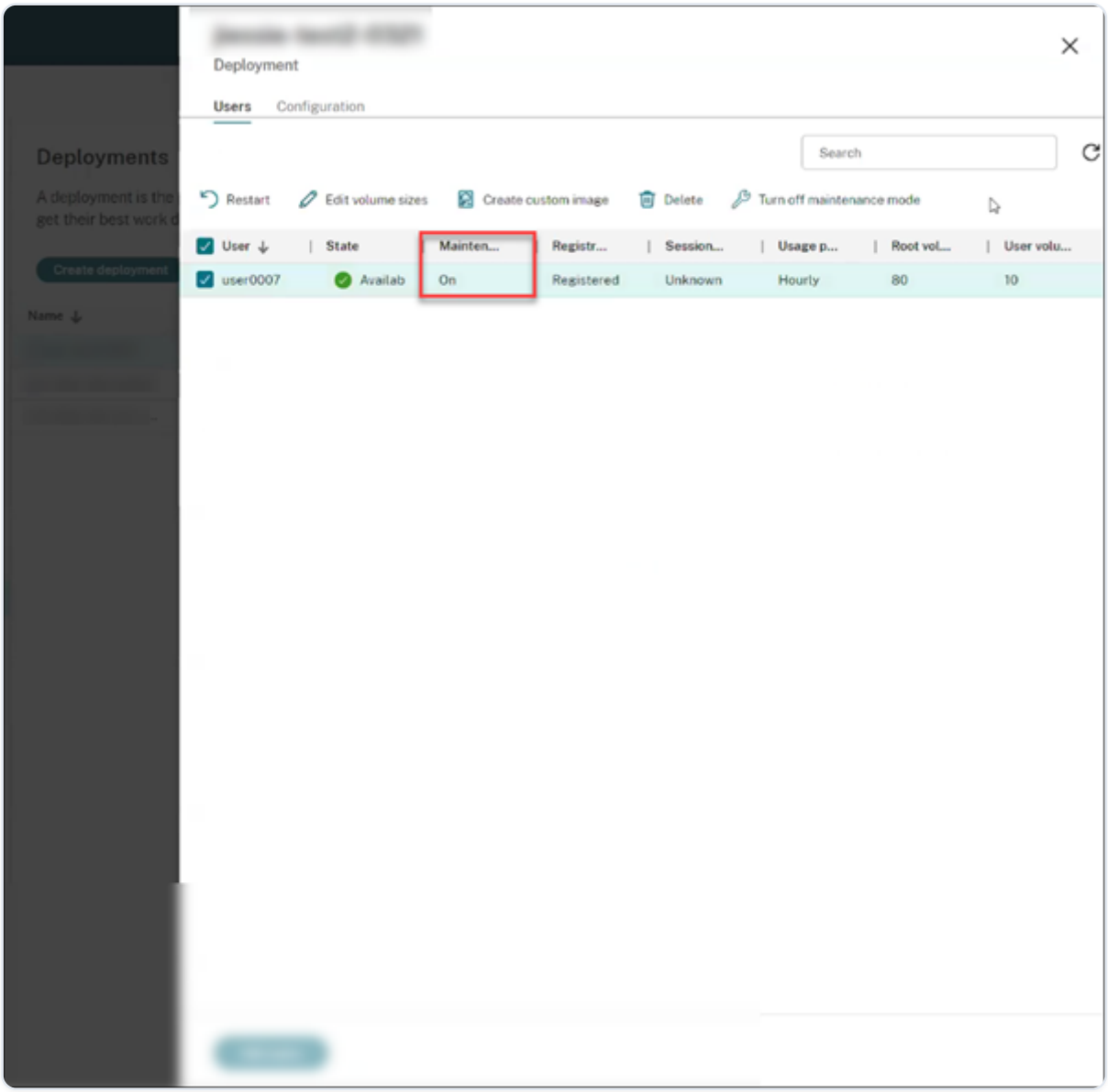
Para criar uma imagem personalizada para um usuário:

1. Em **Web Studio > Quick Deploy > Amazon WorkSpaces Core**, selecione **Deployments**.
2. Selecione a implantação que contém as máquinas que você deseja gerenciar e clique em **Ver detalhes**.
3. No painel **Implantação**, na guia **Usuários**, selecione o **Usuário** cujo estado do espaço de trabalho está disponível e clique em **Criar imagem personalizada**.



> **Nota:**
>
> Você pode criar uma imagem personalizada apenas para a implantação cujo estado do espaço de trabalho está disponível.

4. No painel **Criar imagem personalizada**:
    - Verifique as informações de **Propriedades da imagem**, **SO** e **Conta** do usuário selecionado.
    - Observe a mensagem de aviso que indica o tempo que a implantação da área de trabalho estará em modo de manutenção durante o processo.
    - Preencha os campos obrigatórios como **Nome da imagem** e **Descrição**. O campo **Nome da imagem** sugere os caracteres permitidos para nomes de imagem.
5. Clique em **Criar**. A janela do nó **Imagens** é aberta.
6. Clique no botão **Atualizar**. A imagem personalizada recém-criada é listada com o **Status** como **Pendente**.
7. Selecione a imagem personalizada e clique em **Ver Detalhes**. A janela Imagem é aberta com detalhes como **Status**, **Conta**, **ID**, **SO** e **Descrição**.
8. Clique em **Implantações** na navegação à esquerda. O **Status** da nova implantação é exibido como **Atualizando**.
9. Selecione a nova implantação e clique em **Ver detalhes**.
    - No painel **Implantação**, a guia **Manutenção** é exibida como **Ativada**.



Como prática recomendada:

- Use uma Virtual Private Cloud (VPC) separada que não esteja conectada ao seu ambiente de produção.
- Para Windows WorkSpaces, evite configurar quaisquer Objetos de Política de Grupo (GPOs) antes de criar a imagem. Para obter mais informações, consulte Práticas recomendadas.
- Use um AD Connector dedicado para a criação da imagem.
- Use uma OU dedicada no Active Directory para a criação da imagem. Para obter mais informações, consulte Práticas recomendadas para a criação bem-sucedida de imagens BYOL para Amazon WorkSpaces.

Criar uma implantação

Uma implantação é um grupo de desktops que os usuários podem acessar de sua loja. Este procedimento especifica as características das máquinas virtuais a serem implantadas como desktops e quais usuários do AD podem usá-las.

> **Nota:**
>
> O nome do computador é definido pela Amazon quando o workspace é criado e é usado como um identificador para garantir dados precisos do workspace. Você não pode modificar o nome do computador usando o Citrix DaaS para Amazon Workspaces Core.

Pré-requisitos

Conclua todas as etapas listadas em Preparar e criar uma implantação.

1. Em **Web Studio > Quick Deploy > Amazon WorkSpaces Core > Deployments**, clique em **Create deployment**.
2. Na página **Image and performance**,
   a. se você selecionar uma tenancy dedicada, como a conexão de Diretório, a lista suspensa de imagens listará as imagens que possuem tenancy dedicada. Imagens com tenancy dedicada suportam apenas sessões únicas.
   b. se você selecionar uma tenancy compartilhada como a conexão de Diretório, então o menu suspenso Imagem lista as imagens que têm tenancy Padrão. Imagens com tenancy Compartilhada suportam sessões únicas e múltiplas.
   c. Selecione os **Tamanhos de volume de desempenho** e **raiz**. Clique em **Avançar: Criptografia**.
3. **Criptografia**: Na seção **Selecionar preferência de chave de criptografia**:
   a. A opção **Usar chave KMS gerenciada pela AWS** é selecionada por padrão. Isso criptografa os volumes raiz e de usuário e é gerenciado pela AWS.
   b. Se você selecionar a opção **Usar chave gerenciada pelo cliente**, certifique-se de criar a chave primeiro em **Gerenciamento de Chaves da AWS**. Uma vez criada, insira a chave no campo **Alias da Chave** e clique em **Avançar: Desktops**.

> **Nota:**

> As chaves de criptografia podem ser encontradas no console do **Key Management Service (KMS)** em **Chaves gerenciadas pela AWS** ou **Chaves gerenciadas pelo cliente**.

4. **Desktops**:
    a. Uma nova opção para selecionar **Criar desktops sem atribuir usuários** foi adicionada. Se você selecionar esta opção, é recomendável configurar o local do perfil do usuário para ser armazenado na unidade D: ou em um local externo. Por padrão, o perfil do usuário é armazenado na unidade C:. Os dados e configurações do usuário na unidade C: são perdidos se você reconstruir o WorkSpace. Especifique o número de desktops que você deseja adicionar à implantação. O **Tipo de atribuição de desktop** para esta opção é **Pool aleatório não atribuído**. Clique em **Avançar: Resumo**.

> **Nota:**
>
> A opção **Criar desktops sem atribuir usuários** não está disponível para imagens com aplicativos fornecidos pela AWS. Portanto, você deve atribuir usuários ao criar desktops.

    a. Se você selecionar a opção existente **Atribuir usuários ao criar desktops**, pesquise e selecione os usuários que terão permissão para acessar os desktops. Se você quiser personalizar os tamanhos de volume para um usuário, selecione **Editar tamanhos de volume de usuário e raiz** e, em seguida, especifique os tamanhos. O **Tipo de atribuição de desktop** para esta opção é **Estático pré-atribuído**. Clique em **Avançar: Resumo**.

5. **Resumo:** Revise as informações fornecidas e forneça um **Nome de implantação**. Clique em **Criar implantação**. A página **Implantação** mostra a nova coluna **Desktops** com os detalhes do desktop atribuído.
6. Ressincronizar: Clique em Ressincronizar para uma implantação que está no estado Pendente ou se o número de máquinas listadas em uma implantação não corresponder ao número de máquinas listadas na AWS.
7. Selecione uma implantação e clique em **Ver detalhes**. A página de detalhes da implantação mostra três abas:
    a. **Desktops**: Selecione uma área de trabalho e as configurações a serem modificadas serão exibidas.

b. **Aplicações**: Esta guia permite adicionar novas aplicações e excluir as aplicações existentes. Para obter mais informações sobre como adicionar aplicações a uma implantação existente, consulte Etapa 6. Aplicações.

c. **Usuários**: Esta guia está disponível apenas para implantações não atribuídas para atribuir usuários ou grupos para iniciar a área de trabalho. Clique em **Adicionar**. Atualize as configurações necessárias e clique em **Localizar agora**. Você pode selecionar mais de um usuário na tabela e clicar em **Ok > Concluído**. Você pode adicionar mais usuários e também excluir um usuário existente selecionando as opções apropriadas.

d. **Configuração**: Esta guia mostra o tipo de atribuição da área de trabalho selecionada. Se for uma área de trabalho não atribuída, o **tipo de atribuição da área de trabalho** será **Pool aleatório não atribuído**.

Integrar aplicativos do Microsoft 365 Windows

Para integrar os Aplicativos do Microsoft 365, consulte Aplicativos do Microsoft 365 para empresas agora disponíveis nos serviços Amazon WorkSpaces e Microsoft 365 Bring Your Own License (BYOL).

Gerenciar máquinas em uma implantação

Além dos recursos de gerenciamento de máquinas descritos em Gerenciar catálogos de máquinas, para algumas ações, você pode selecionar máquinas para gerenciar a partir de uma implantação.

Para gerenciar máquinas em uma implantação:

1. Em **Web Studio > Quick Deploy > Amazon WorkSpaces Core**, selecione **Implantações**.
2. No painel **Implantações**, selecione a implantação que contém as máquinas que você deseja gerenciar.
3. Clique em **Exibir detalhes**.
4. No painel **Detalhes da implantação**, selecione a máquina que você deseja gerenciar.
5. Nas ações exibidas, selecione a ação que você deseja executar na máquina:

- Clique em **Editar tamanho do volume** para alterar o tamanho do volume da máquina.
- Clique em **Excluir** para excluir a máquina da implantação e da AWS. Se uma máquina estiver em um grupo de entrega, ela só poderá ser excluída se estiver no modo de manutenção.
- Clique em **Ativar/desativar modo de manutenção** para ativar o modo de manutenção (se estiver desativado) ou desativá-lo (se estiver ativado) para a máquina.

Adicionar aplicativos a uma implantação

Para adicionar aplicativos a uma implantação existente:

1. Em **Web Studio > Quick Deploy > Amazon WorkSpaces Core**, selecione Implantações.
2. No painel Implantações, selecione a implantação à qual você deseja adicionar os aplicativos.
3. Clique em Adicionar aplicativos. O painel Adicionar Aplicativo é aberto.
4. Clique no menu Adicionar e selecione uma das seguintes fontes para adicionar os aplicativos:
    - Do menu Iniciar
    - Manualmente
    - Pacotes de aplicativos
    - Existente
    - Grupo de aplicativos

Para obter mais informações sobre como adicionar aplicativos a uma implantação existente, consulte Etapa 6. Aplicativos.

Usar desktops persistentes com um perfil de usuário não persistente

O Workspace Environment Management™ pode ser usado para configurar as definições do Profile Management para ativar desktops persistentes com perfis de usuário não persistentes. Isso proporciona uma experiência de desktop personalizável, mantendo o gerenciamento fácil e o armazenamento centralizado dos perfis de usuário, criando uma solução flexível e escalável para ambientes de desktop virtual. Faça o seguinte para configurar a definição:

1. No console do WEM, navegar para **Configuration Set > Policies and Profiles > Citrix Profile Management Settings**.
2. Selecione **Enable Profile Management Configuration** e navegar para a guia **Profile Handling**.
3. Selecione **Delete locally cached profiles on logoff**.

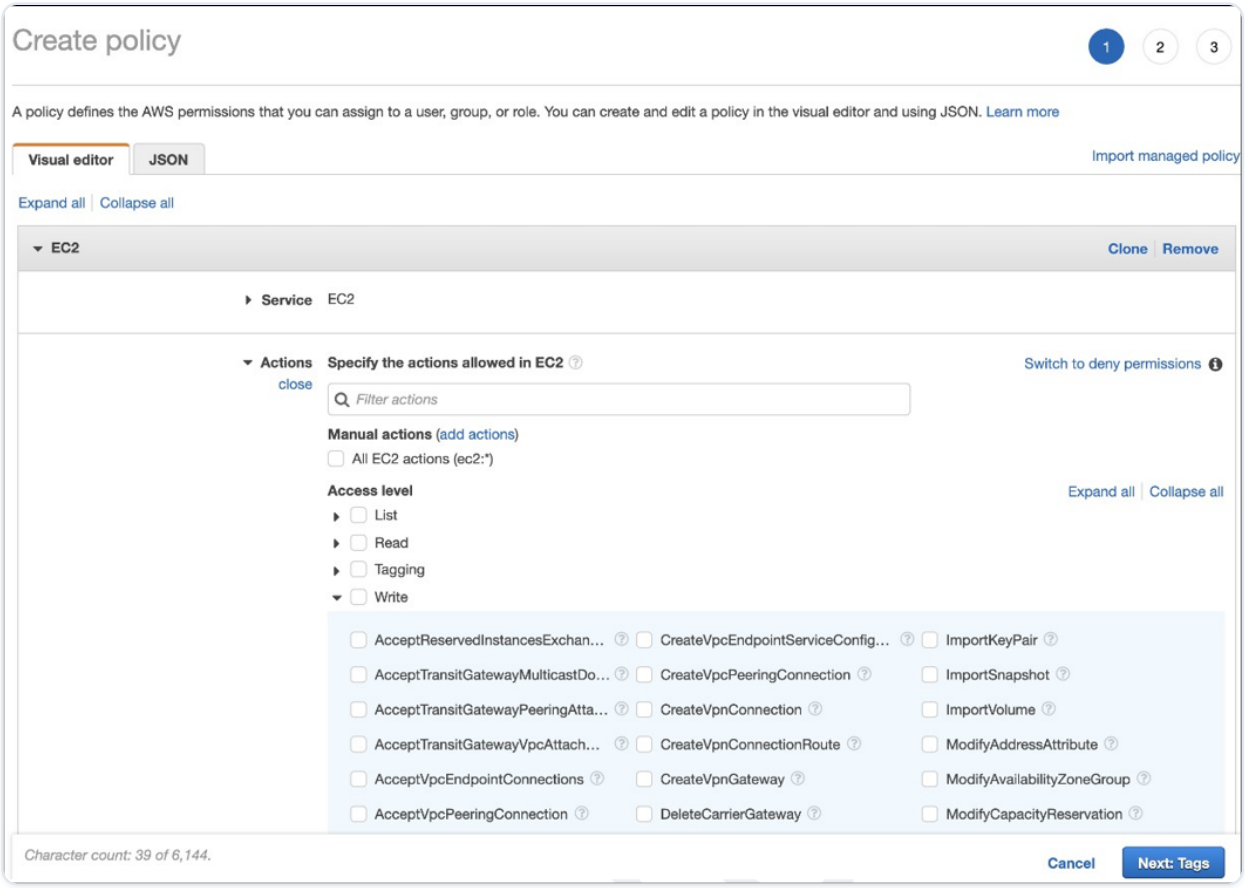
Referência

Permissões de acesso programático da conta AWS

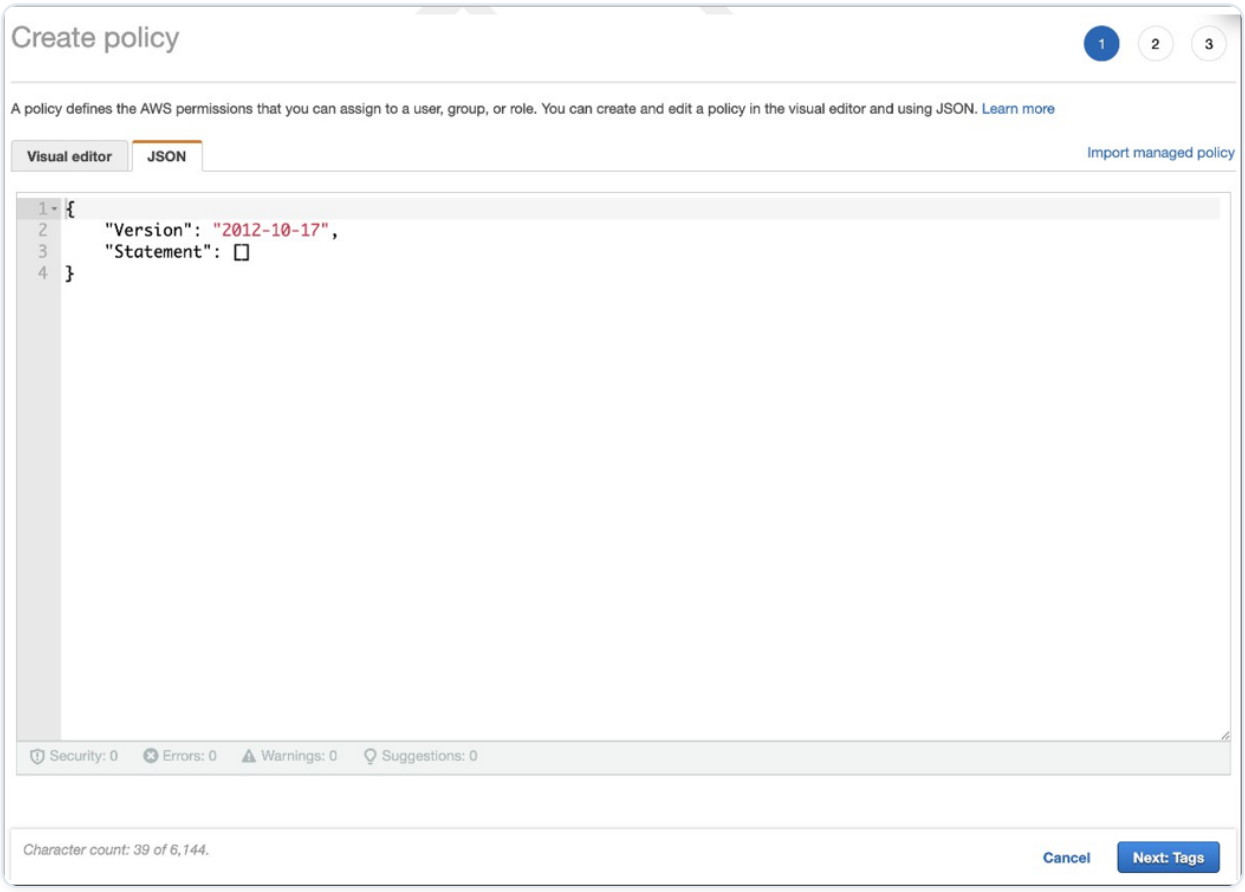
A conta de usuário AWS deve ter certas permissões de acesso programático para fazer chamadas de API para a camada de recursos da AWS. O acesso programático cria um ID de chave de acesso e uma chave de acesso secreta. Você pode criar uma política contendo essas permissões

no console do IAM. Conforme mostrado nos gráficos a seguir, você pode usar o editor visual (adicionando as permissões uma a uma) ou o JSON (adicionando o trecho abaixo). Para obter mais informações, consulte Criando um usuário IAM em sua conta AWS.

- Na guia **Visual editor**, adicione as permissões uma a uma.



- Na guia **JSON**, adicione o trecho mostrado após o gráfico a seguir.



Permissões necessárias

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Sid": "VisualEditor0",

            "Effect": "Allow",

            "Action": [

                    "workdocs:DeregisterDirectory",

                    "workdocs:RegisterDirectory",

                    "workdocs:AddUserToGroup",
```

```
                "ec2:ImportInstance",
                "ec2:DescribeImages",
                "ec2:DescribeImageAttribute"
                "ec2:CreateKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:ModifyImageAttribute",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:RunInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateTags",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInternetGateways",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeInstanceTypes",
                "servicequotas:ListServices",
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:ListTagsForResource",
                "servicequotas:GetServiceQuota",
                "servicequotas:GetAssociationForServiceQuotaTemplate",
                "servicequotas:ListAWSDefaultServiceQuotas",
                "servicequotas:ListServiceQuotas",
```

```
                    "servicequotas:GetAWSDefaultServiceQuota",

"servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",

"servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",

"servicequotas:ListRequestedServiceQuotaChangeHistory",

"servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
                    "sts:DecodeAuthorizationMessage",
                    "ds:*",
                    "workspaces:*",
                    "iam:GetRole",
                    "iam:GetContextKeysForPrincipalPolicy",
                    "iam:SimulatePrincipalPolicy"


                ],
                "Resource": "*"
            }
        ]
}
```

Citrix DaaS™ para Google Cloud

Com o Studio, você pode implantar e gerenciar aplicativos e desktops virtuais no Google Cloud. Para obter informações sobre os recursos suportados, consulte a matriz de recursos do Citrix Virtual Apps and Desktops.

Para implantar e gerenciar aplicativos e desktops do Google Cloud usando o Studio, siga estas etapas:

1. Peça o Citrix DaaS para Google Cloud no Google Cloud Marketplace.
2. Faça login no Citrix Cloud.
3. No bloco **DaaS**, clique em **Gerenciar** para abrir o Studio.
4. Implante aplicativos e desktops virtuais usando um destes fluxos de trabalho fornecidos na seção **Gerenciar**:

    - Implantação Rápida (recomendado para implantação rápida e guiada). Para obter mais informações, consulte Implantação Rápida para Google Cloud.

        > **Nota:**
        >
        > Para realizar configurações avançadas ou opções de gerenciamento, converta sua implantação para o modo de configuração completa. Para obter mais informações, consulte Converter uma implantação.

    - Configuração Completa (recomendado para requisitos de configuração avançada). Para obter mais informações, consulte Introdução: Planejar e construir uma implantação.

> **Nota:**
>
> Para obter instruções passo a passo sobre como implantar e configurar aplicativos e desktops virtuais no Google Cloud, consulte este artigo do Citrix Tech Zone: Virtualização Citrix no Google Cloud. Este artigo aborda a definição da arquitetura de implantação, a preparação do projeto do Google Cloud, a configuração de serviços de rede e a implantação do Active Directory.

Implantação Rápida para Google Cloud

A Implantação Rápida para Google Cloud oferece uma experiência de usuário simplificada para conectar o Citrix DaaS ao Google Cloud e criar uma implantação de aplicativos e desktops virtuais. Sua interface de usuário otimizada guia os administradores pelas etapas principais dessa jornada e remove complicações desnecessárias.

Esta interface oferece configuração básica, sem recursos avançados.

Para implantar aplicativos e desktops virtuais usando o Quick Deploy, siga o assistente na tela para concluir estas etapas:

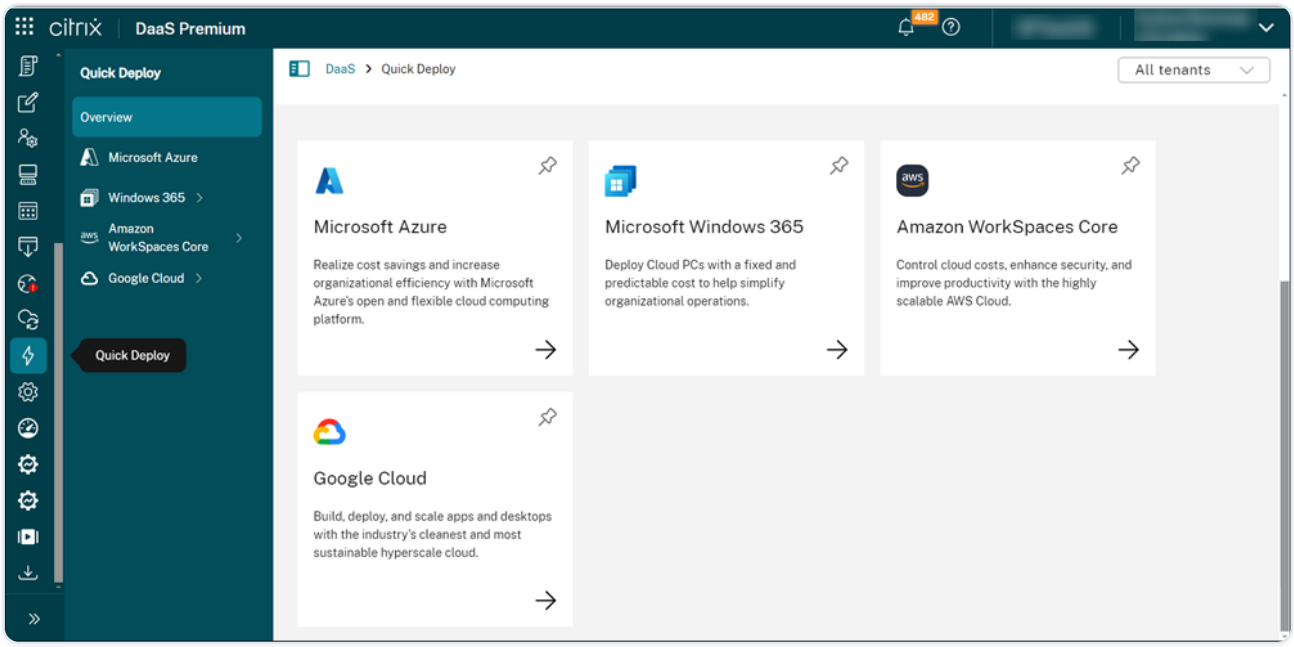
1. Iniciar o Quick Deploy para Google Cloud
2. Criar um local de recurso
3. Adicionar um projeto do Google Cloud
4. Criar uma conexão de rede
5. Criar uma implantação

Depois de criar uma implantação, execute estas tarefas conforme necessário:

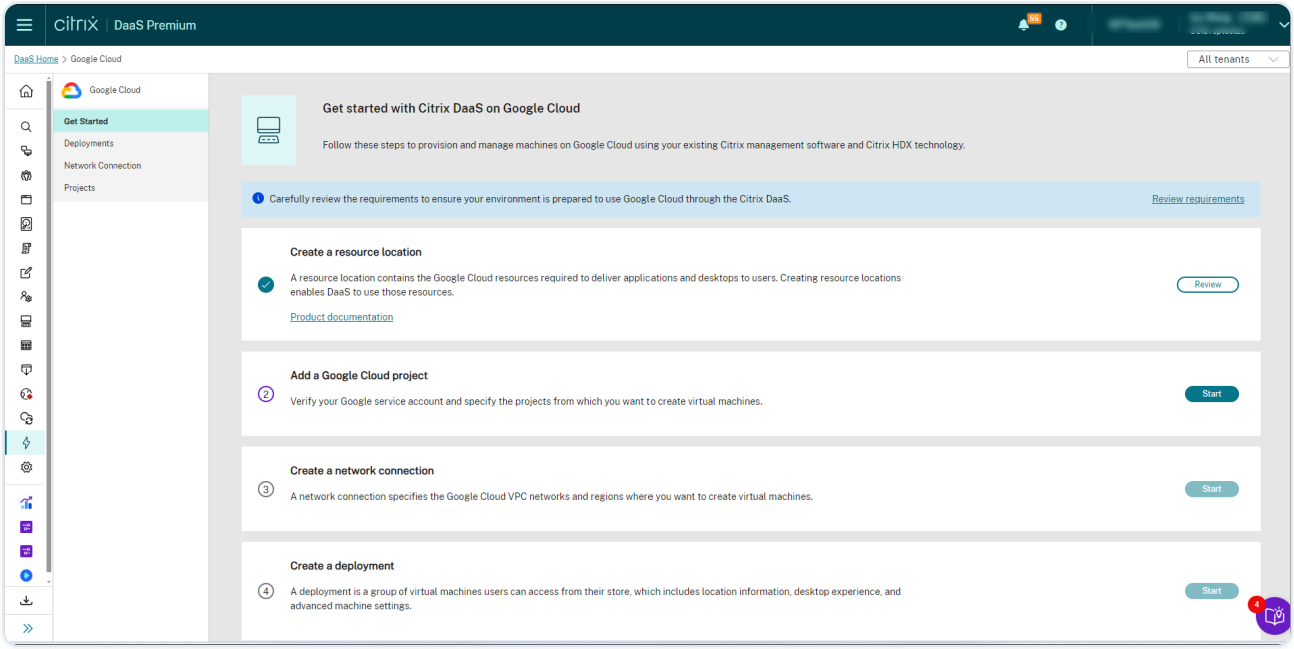
- Conceder direitos de acesso aos usuários
- Converter uma implantação para o modo de configuração completa para configurações avançadas e opção de gerenciamento.

Iniciar o Quick Deploy para Google Cloud

O Quick Deploy para Google Cloud pode ser acessado de dentro do Studio, selecionando o nó Quick Deploy.

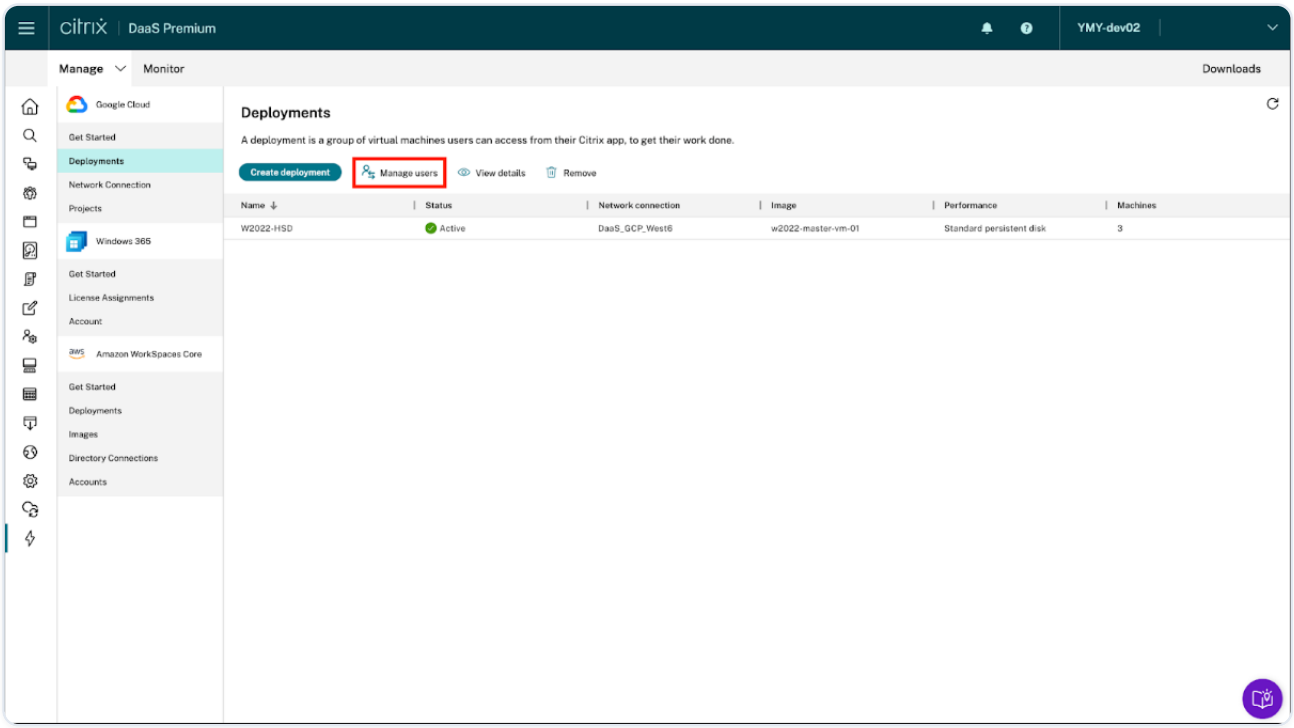


Para iniciar o processo do Quick Deploy, revise as etapas fornecidas na página Introdução. Comece com **Revisar requisitos**.



Gerenciar direitos de acesso do usuário

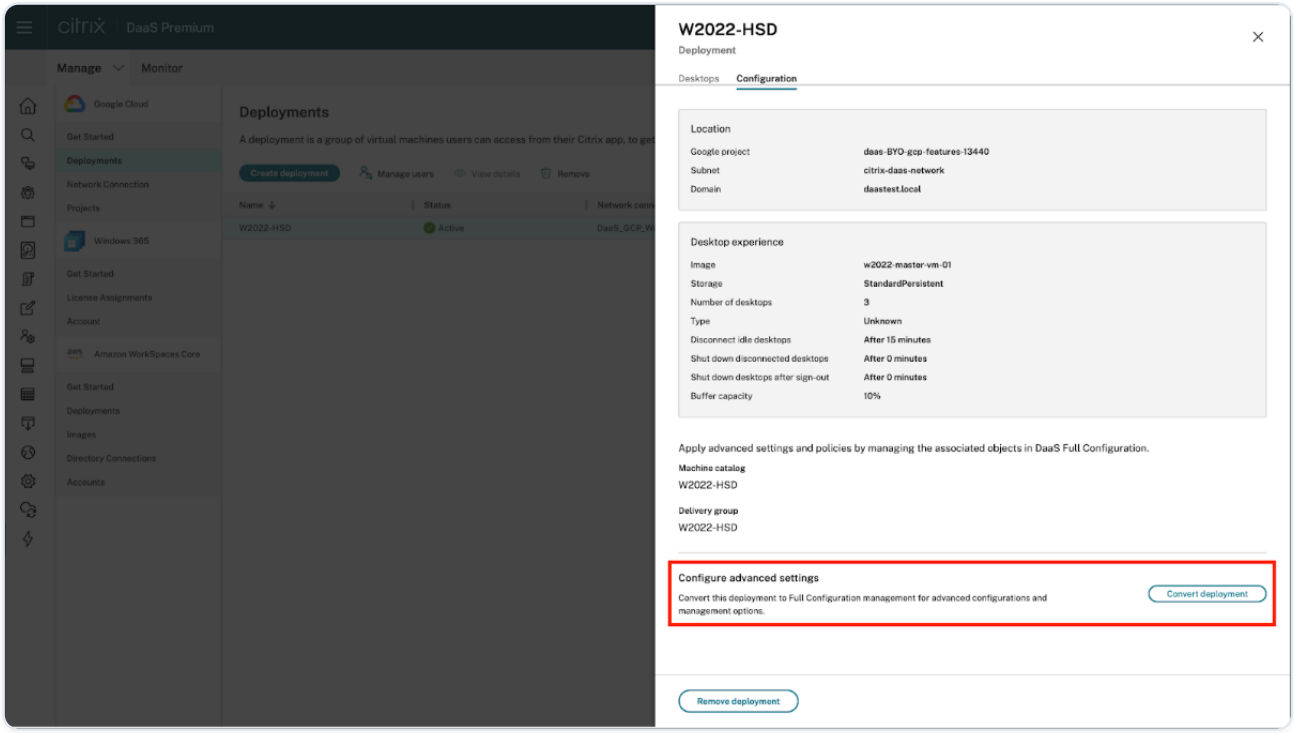
Após a criação de uma implantação, conceda permissões de acesso aos usuários conforme necessário. Para concluir esta tarefa, selecione a implantação respectiva e, em seguida, selecione **Gerenciar usuários**.



Converter uma implantação

Antes de realizar quaisquer configurações avançadas ou atividades de gerenciamento, certifique-se de converter as implantações. Para converter uma implantação:

1. Clique em **Implantações** na navegação à esquerda.
2. Selecione uma implantação e clique em **Exibir detalhes**.
3. Clique na guia **Configuração** e selecione **Converter implantação**.

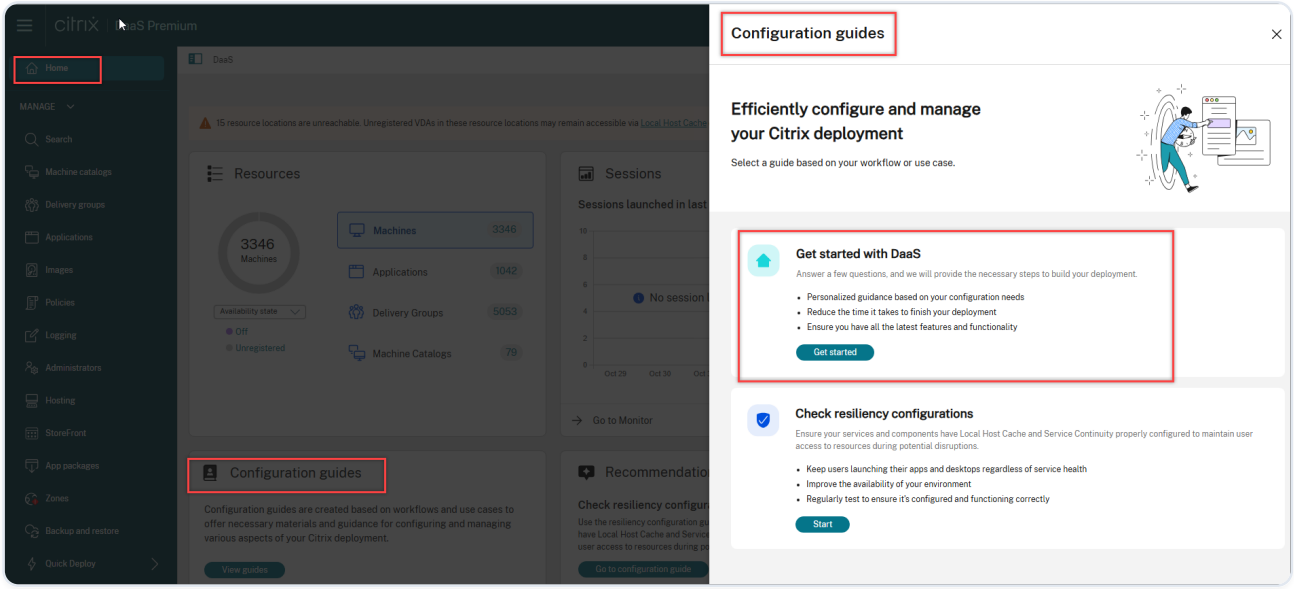


Nota:

Uma vez que uma implantação é convertida, a ação é irreversível e as implantações convertidas não aparecem mais no Quick Deploy.

Usar o guia de primeiros passos do DaaS

O guia de primeiros passos do DaaS otimiza e simplifica o processo de implantação do DaaS para administradores novos e experientes. Usando o guia, você pode configurar rapidamente suas implantações DaaS respondendo a uma série de perguntas.



Este artigo o guiará pelos processos de configuração de cinco cenários típicos de implantação do DaaS.

Benefícios

Os benefícios de usar este guia incluem:

- **Fácil de começar**. Este guia conecta as etapas essenciais de implantação por meio de um fluxo de trabalho passo a passo guiado por questionário. Se você é um novo administrador, pode configurar rapidamente sua implantação enquanto aprende conceitos e terminologia por meio de ajuda contextual.
- **Simplifique configurações complexas**. Este guia fornece configurações pré-configuradas sempre que necessário e fornece acesso ao Studio para configurações avançadas. Se você é um administrador experiente, pode usar o guia como ponto de partida para configurações complexas.

Cenários de implantação compatíveis

Este guia oferece implantações rápidas para estes cenários:

O QUE ENTREGAR?	AS MÁQUINAS JÁ EXISTEM?	TIPO DE MÁQUINA	OBSERVAÇÃO
Aplicativos e desktops virtuais	Não	Máquinas virtuais (Provisionadas por DaaS)	Gerenciamento de energia
Aplicativos e desktops virtuais	Sim	Máquinas virtuais ou PCs blade	Gerenciamento de energia
Aplicativos e desktops virtuais	Sim	Máquinas físicas ou virtuais	Sem gerenciamento de energia
PCs de escritório	Sim	Máquinas físicas	Gerenciamento de energia
PCs de escritório	Sim	Máquinas físicas	Não gerenciado por energia

Consulte as seções a seguir para obter instruções detalhadas:

- Entregar aplicativos e desktops do zero (gerenciado por energia)
- Entregar aplicativos e desktops usando máquinas existentes (gerenciado por energia)
- Entregar aplicativos e desktops usando máquinas existentes (não gerenciado por energia)
- Entregar PCs de escritório (gerenciado por energia)
- Entregar PCs de escritório (não gerenciado por energia)

Terminologia

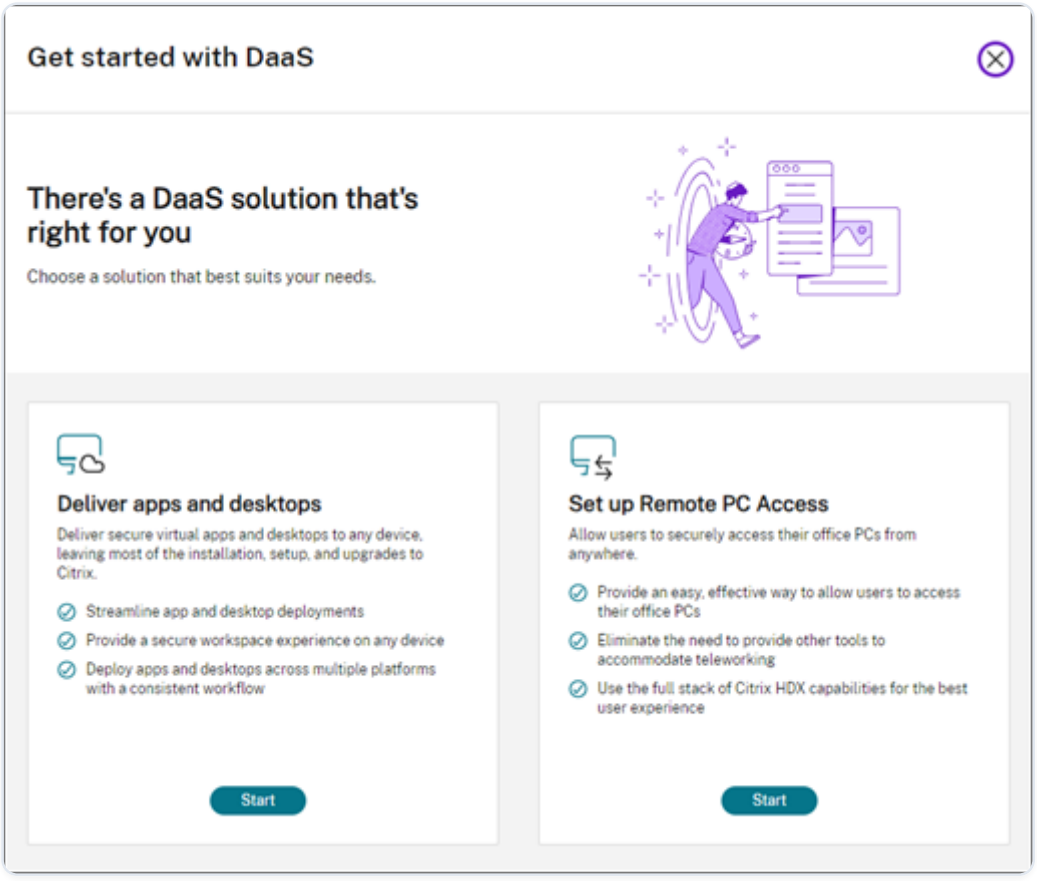
A seguir estão os termos específicos do DaaS:

- **Local de recurso.** Contém os recursos necessários para entregar aplicativos e desktops aos usuários.
- **Conexão de host.** Conecta o DaaS a um host (hipervisor ou serviço de nuvem) em um local de recurso. A criação de conexões de host é necessária quando você deseja criar e gerenciar máquinas em hosts ou gerenciar a energia de máquinas existentes.

- **Imagem mestre.** Serve como um modelo para replicar máquinas virtuais em seu host. Inclui o sistema operacional, aplicativos, Virtual Delivery Agent (VDA) e outros softwares.
- **Catálogo de máquinas.** Coleção de máquinas idênticas. Elas podem ser virtuais ou físicas, dependendo das suas necessidades. Você pode criar um catálogo de máquinas para criar máquinas configuradas de forma idêntica em um host ou importar máquinas para o DaaS para gerenciamento.
- **Grupo de entrega.** Contém máquinas de catálogos de máquinas. Além disso, especifica quais usuários podem usar essas máquinas e quais aplicativos e desktops estão disponíveis para esses usuários.
- **Perfil de Máquina.** Especifica as propriedades das máquinas virtuais. As VMs em um catálogo podem herdar propriedades de um perfil de máquina.

Acessar o guia

1. Vá para a página **DaaS > Início**.
2. Localize **Introdução ao DaaS**.
3. Clique em **Introdução** para iniciar seu processo de implantação.



Nota:

> Você pode sair do processo a qualquer momento clicando em **Fechar** e o guia salva suas configurações automaticamente. Para continuar sua configuração, clique em **Continuar**. Para começar do zero, clique em **Recomeçar**.

Entregar aplicativos e desktops do zero (com gerenciamento de energia)

Esta seção o guiará pelo processo de implantação de criação de VMs e entrega de aplicativos e desktops usando-as.

Pré-requisitos

Antes de começar, você precisa:

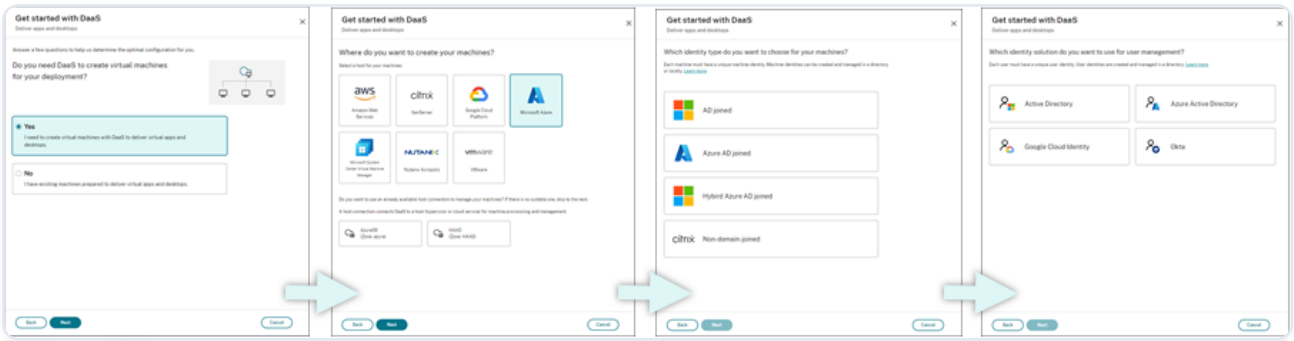
- Conectividade do Citrix Cloud™ com o provedor de identidade de destino

  Para obter mais informações, consulte a seção correspondente em Provedores de identidade.
- Função: Administrador Completo ou Administrador de Nuvem
- Permissões necessárias no hipervisor de destino ou serviço de nuvem.

  Para obter mais informações, consulte as seções correspondentes em Criar e gerenciar conexões.
- Credenciais de administrador para criação de conta de VM

Preparação

Responda às perguntas na tela para concluir as seguintes configurações de nível de infraestrutura. Consulte a tabela a seguir para obter detalhes.

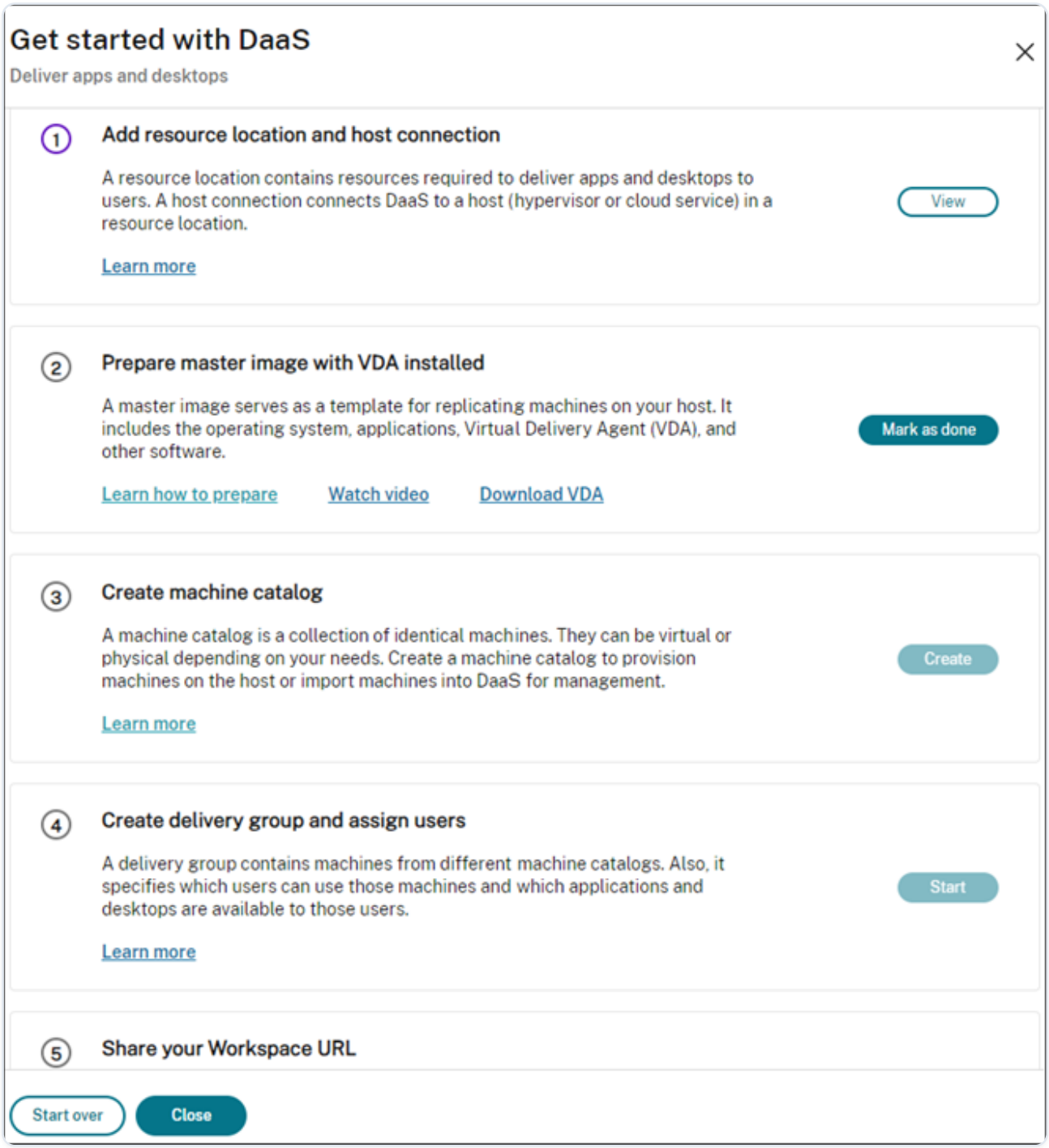


#	CONFIGURAÇÃO	DESCRIÇÃO
1	Especifique se a criação de VM é necessária	Selecione **Sim**.

#	CONFIGURAÇÃO	DESCRIÇÃO
2	Selecione o tipo de host	Selecione um tipo de host para sua implantação.
		Opções: AWS, XenServer (anteriormente Citrix Hypervisor™), Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis e VMware
3	Selecione o tipo de identidade da máquina	Selecione um tipo de identidade para o gerenciamento da máquina.
		Opções: ingressado no AD, ingressado no Microsoft Entra, ingressado no Microsoft Entra híbrido e não ingressado no domínio
4	Selecione o tipo de identidade do usuário	Selecione um tipo de identidade para o gerenciamento do usuário.
		Opções: Active Directory, Microsoft Entra ID, Google Cloud Identity e Okta

Etapas de implantação

Depois de concluir as configurações de nível de infraestrutura, as etapas específicas para este cenário de implantação aparecem da seguinte forma.



Siga as instruções na tela para concluir as configurações.

Passo 1: Adicionar um local de recurso e conexões de host

Configure seu local de recurso instalando os Cloud Connectors e configure as conexões para hipervisores ou serviços de nuvem no local.

1. Nomeie o local de recurso.
2. Baixe e instale os Cloud Connectors em pelo menos duas máquinas Windows Server.
3. Detecte os Cloud Connectors instalados.

4. Adicione e configure conexões de host para o local de recurso. As configurações detalhadas de uma conexão incluem:

   - Detalhes da conexão, como o endereço da conexão, nome de usuário e senha.
   - Recursos de armazenamento
   - Recursos de rede

> **Nota:**
>
> O DaaS cria e gerencia VMs em hosts por meio dessas conexões. Você deve especificar as conexões ao criar catálogos de máquinas.

Passo 2: Prepare imagens mestre para suas máquinas

Prepare imagens mestre em VMs em seu local de recurso. Para obter mais informações, consulte Preparar uma imagem mestre no hipervisor ou serviço de nuvem.

Passo 3: Criar catálogos de máquinas

Crie um catálogo de máquinas para criar um grupo de máquinas configuradas de forma idêntica em um host. As etapas detalhadas são as seguintes:

1. Nomeie o catálogo.
2. Selecione o tipo de máquina.

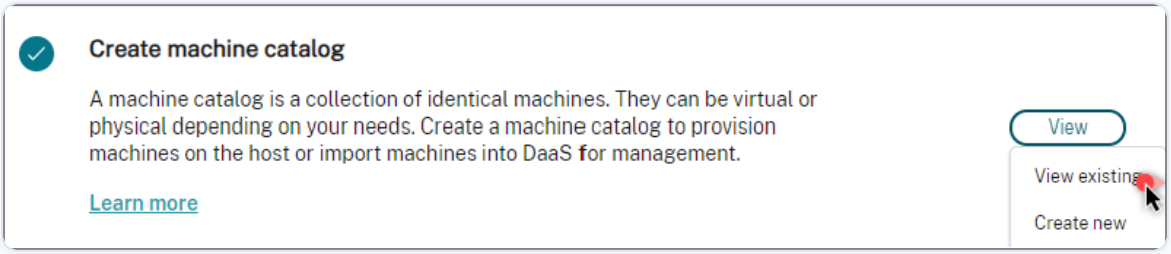
   Opções: Multi-sessão, Sessão única estática (desktops pessoais) e Sessão única aleatória (desktops agrupados).
3. Selecione uma conexão de host.

   As opções são originadas de todas as conexões de host que você configurou para seus locais de recurso na Etapa 1.
4. Selecione uma imagem mestre.
5. Selecione um perfil de máquina.

> **Nota:**
>
> O suporte a perfil de máquina está atualmente disponível para serviços de nuvem Azure, GCP e AWS, e o uso de perfil de máquina é opcional para GCP.

6. Defina quantas máquinas você deseja criar.
7. Defina as identidades da máquina.

   Por padrão, o tipo de identidade da máquina que você selecionou na fase de preparação é exibido. Forneça as configurações de identidade necessárias para as VMs, como domínio, OU e esquema de nomenclatura.
8. Insira as credenciais de administrador necessárias para a criação da máquina.
9. Clique em **Criar**.

> **Dica:**
>
> O botão **Criar** fica disponível somente depois que você fornece todas as configurações necessárias.
>
> Para visualizar o progresso da criação do catálogo, selecione **View > View existing**.
>
> 
>

Etapa 4: Criar grupos de entrega e atribuir usuários

> **Dica:**
>
> Antes de criar grupos de entrega, visualize os catálogos existentes para garantir que pelo menos um catálogo tenha sido criado com êxito. Caso contrário, você será impedido de criar grupos de entrega.
>
> A criação de um grupo de entrega inclui as seguintes subtarefas:

- Adicionar VMs ao grupo
- Atribuir usuários ao grupo
- Especificar quais aplicativos e desktops você deseja disponibilizar para os usuários atribuídos

1. Nomear o grupo.

2. Adicione máquinas ao grupo selecionando um catálogo de máquinas e especificando quantas VMs estão disponíveis para o grupo.
3. Especifique os aplicativos e desktops disponíveis para este grupo:
    - Para adicionar aplicativos de uma máquina em execução no catálogo selecionado, clique em **Add new > From start menu**.
    - Para adicionar aplicativos implantados em compartilhamentos de rede, clique em **Add new > Manually** e, em seguida, forneça as configurações necessárias, como caminho, diretório de trabalho e muito mais.
    - (Visível apenas com máquinas de SO de várias sessões) Para entrega de desktop, mantenha **Enable desktop delivery** selecionado.
4. Adicione usuários que podem acessar aplicativos e desktops neste grupo.

Etapa 5: Compartilhe a URL da loja com seus usuários

Vá para **StoreFront Cloud \> Acesso** e, em seguida, compartilhe a URL da loja com seus usuários.

Entregue aplicativos e desktops usando máquinas existentes (com gerenciamento de energia)

Esta seção o guia pelo processo de implantação de entrega de aplicativos e desktops usando máquinas existentes (com gerenciamento de energia).

Pré-requisitos

Antes de começar, você precisa:

- Conectividade do Citrix Cloud com o provedor de identidade de destino

  Para obter mais informações, consulte a seção correspondente em Provedores de identidade.
- Função: Administrador Completo ou Administrador da Nuvem

Preparação

Responda às perguntas na tela para concluir as seguintes configurações de nível de infraestrutura.

#	CONFIGURAÇÃO	DESCRIÇÃO
1	Especifique se a criação de VM é necessária	Selecione **Não**.
2	Selecione se o gerenciamento de energia é necessário	Selecione **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade)**.
3	Selecione a plataforma de host	Selecione a plataforma de host onde suas máquinas existentes residem.
		Opções: AWS, Citrix®, Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis e VMware
4	Selecione o tipo de identidade do usuário	Selecione um tipo de identidade para gerenciamento de usuários.
		Opções: Active Directory, Microsoft Entra ID, Google Cloud Identity e Okta

Etapas de implantação

Depois de concluir as configurações de nível de infraestrutura, as etapas específicas para este cenário de implantação aparecerão. Siga as instruções na tela para concluir as configurações.

Etapa 1: Adicionar um local de recurso e conexões de host

Configure seu local de recurso instalando os Cloud Connectors e configure as conexões com hipervisores ou serviços de nuvem em seu local.

1. Nomeie o local de recurso.
2. Baixe e instale os Cloud Connectors em pelo menos duas máquinas Windows Server.
3. Detectar Cloud Connectors instalados.

4. Adicione e configure conexões de host para o local de recurso. Exemplos de configurações de conexão incluem o endereço de conexão, nome de usuário e senha.

> **Nota:**
>
> O DaaS gerencia o consumo de energia das máquinas em locais de recurso por meio de conexões. Você precisa especificar uma conexão ao importar suas máquinas para um catálogo.

Etapa 2: Criar catálogos de máquinas

Crie um catálogo de máquinas e importe suas máquinas para ele.

1. Nomeie o catálogo
2. Selecione o tipo de máquina.

   Opções: Multi-sessão, Sessão única estática (desktops pessoais) e Sessão única aleatória (desktops agrupados).
3. Selecione um local de recurso.
4. Importe máquinas para o catálogo. As máquinas são organizadas por conexão de host. Escolha uma conexão de host para importar as máquinas associadas.
5. Clique em **Criar**.

Etapa 3: Crie grupos de entrega e atribua usuários

Para criar um grupo de entrega, você deve:

- Adicionar VMs ao grupo
- Atribuir usuários ao grupo
- Especifique quais aplicativos e desktops você deseja disponibilizar para os usuários atribuídos

1. Nomeie o grupo.
2. Selecione um catálogo de máquinas conforme necessário e, em seguida, especifique quantas máquinas estão disponíveis para o grupo de entrega.
3. Especifique os aplicativos e desktops disponíveis para este grupo:

   - Para adicionar aplicativos de uma máquina em execução no catálogo selecionado, clique em **Adicionar novo > Do menu Iniciar**.

- Para adicionar aplicativos implantados em compartilhamentos de rede, clique em **Adicionar novo > Manualmente** e, em seguida, forneça as configurações necessárias, como caminho, diretório de trabalho e muito mais.
- (Visível apenas com máquinas de SO multi-sessão) Para entrega de desktop, mantenha **Habilitar entrega de desktop** selecionado.

4. Adicione usuários ao grupo.

Etapa 4: Compartilhe a URL da loja com seus usuários

Vá para **Citrix® StoreFront Cloud \> Acesso** e, em seguida, compartilhe o URL da loja com seus usuários.

Entregar aplicativos e desktops usando máquinas existentes (não gerenciadas por energia)

Esta seção o orienta pelo processo de implantação de entrega de aplicativos e desktops usando máquinas existentes (não gerenciadas por energia).

Pré-requisitos

Antes de começar, você precisa:

- Conectividade do Citrix Cloud com o provedor de identidade de destino

  Para obter mais informações, consulte a seção correspondente em Provedores de identidade
- Função: Administrador Completo ou Administrador de Nuvem

Preparação

Responda às perguntas na tela para concluir as seguintes configurações de nível de infraestrutura.

#	CONFIGURAÇÃO	DESCRIÇÃO
1	Especifique se a criação de VM é necessária	Selecione **Não**.
2	Selecione se o gerenciamento de energia é necessário	Selecione **Máquinas que não são gerenciadas por energia (por exemplo, máquinas físicas)**.

#	CONFIGURAÇÃO	DESCRIÇÃO
3	Selecione o tipo de identidade do usuário	Selecione um tipo de identidade para gerenciamento de usuários.
		Opções: Active Directory, Microsoft Entra ID, Google Cloud Identity e Okta

Etapas de implantação

Após concluir as configurações de nível de infraestrutura, aparecem as etapas específicas para este cenário de implantação. Siga as instruções na tela para concluir as configurações.

Etapa 1: Adicionar um local de recurso

Configure seu local de recurso instalando os Cloud Connectors.

1. Nomeie o local de recurso.
2. Baixe e instale os Cloud Connectors em pelo menos duas máquinas Windows Server.
3. Detecte os Cloud Connectors instalados.

> **Nota:**
>
> A criação de conexões de host é necessária apenas quando você deseja gerenciar o consumo de energia das máquinas.

Etapa 2: Criar um catálogo de máquinas

Crie um catálogo de máquinas e importe suas máquinas para ele.

1. Nomeie o catálogo
2. Selecione o tipo de máquina.

   Opções: Multissessão, Sessão única estática (desktops pessoais) e Sessão única aleatória (desktops agrupados).
3. Selecione um local de recurso.
4. Importe máquinas para o catálogo.

Para facilitar a pesquisa de máquinas, use nomes de computador parciais e seleção de diretório.

5. Clique em **Criar**.

Etapa 3: Criar grupos de entrega e atribuir usuários

Para criar um grupo de entrega, você deve:

- Adicionar VMs ao grupo
- Atribuir usuários ao grupo
- Especifique quais aplicativos e desktops você deseja disponibilizar para os usuários atribuídos

1. Nomeie o grupo.
2. Selecione um catálogo de máquinas conforme necessário e, em seguida, especifique quantas máquinas estão disponíveis para o grupo de entrega.
3. Especifique os aplicativos e desktops disponíveis para este grupo:
    - Para adicionar aplicativos de uma máquina em execução no catálogo selecionado, clique em **Adicionar novo > Do menu iniciar**.
    - Para adicionar aplicativos implantados em compartilhamentos de rede, clique em **Adicionar novo > Manualmente** e, em seguida, forneça as configurações necessárias, como caminho, diretório de trabalho e muito mais.
    - (Visível apenas com máquinas de SO de várias sessões) Para entrega de desktop, mantenha **Habilitar entrega de desktop** selecionado.
4. Adicione usuários ao grupo.

Etapa 4: Compartilhe a URL da loja com seus usuários

Vá para **Citrix® StoreFront Cloud \> Acesso** e, em seguida, compartilhe a URL da loja com seus usuários.

Entregar PCs de escritório (com gerenciamento de energia)

Esta seção o guiará pelo processo de implantação de entrega de PCs de escritório (com gerenciamento de energia).

Pré-requisitos

Antes de começar, você precisa:

- Nomes das máquinas dos PCs.

- O Citrix Virtual Delivery Agent (VDA) é instalado em cada PC. (Esta etapa pode ser feita após a criação do catálogo.)

  Para obter mais informações, consulte Baixar VDA.

Preparação

Responda às perguntas na tela para concluir as seguintes configurações de nível de infraestrutura.

#	ETAPA	DESCRIÇÃO
1	Selecione o tipo de alocação de máquina.	Selecione como as máquinas são atribuídas.
		Opções: Estático autoatribuído, Estático pré-atribuído e Pool aleatório não atribuído
2	Determine se deve permitir que os usuários liguem as máquinas	Selecione **Quero que os usuários remotos liguem as máquinas por conta própria**.
3	Selecione o tipo de identidade do usuário	Selecione um tipo de identidade para o gerenciamento de usuários.
		Opções: Active Directory, Microsoft Entra ID, Google Cloud Identity e Okta

Etapas de implantação

Depois de concluir as configurações de nível de infraestrutura, as etapas específicas para este cenário de implantação aparecerão. Siga as instruções na tela para concluir as configurações.

Etapa 1: Adicionar um local de recurso e conexões de host

Configure seu local de recurso instalando os Cloud Connectors e adicione uma conexão do tipo **Remote PC Wake on LAN**.

1. Nomeie o local do recurso.

2. Baixe e instale os Cloud Connectors em pelo menos duas máquinas Windows Server.
3. Detecte os Cloud Connectors instalados.
4. Clique em **Adicionar novo** para adicionar uma conexão:
    a. Selecione um local de recurso (zona).
    b. Selecione **Remote PC Wake on LAN** para **Tipo de conexão**.
    c. Insira um nome para a conexão.

> **Nota:**
>
> O DaaS gerencia o consumo de energia das máquinas por meio das conexões configuradas. Você deve configurar conexões do tipo **Remote PC Wake on LAN** ao criar catálogos de Acesso Remoto a PCs para máquinas com gerenciamento de energia.

Etapa 2: Criar um catálogo de Acesso Remoto a PCs

Crie um catálogo de máquinas e importe seus PCs de escritório para ele.

1. Nomeie o catálogo
2. Selecione um local de recurso.
3. Selecione um tipo de alocação de máquina. Por padrão, o tipo selecionado na fase de preparação é exibido.
4. Selecione a **conexão Wake on LAN**. As opções são as conexões do tipo **Remote PC Wake on LAN** que você configurou para o local selecionado.
5. Importe suas máquinas.
6. Clique em **Criar**.

Etapa 3: Criar grupos de entrega e atribuir usuários

Crie um grupo de entrega para agrupar máquinas que você deseja entregar e especificar quem pode acessá-las.

1. Nomeie o grupo.
2. Selecione um catálogo de máquinas conforme necessário. Somente os catálogos de **Acesso Remoto a PCs** aparecem.
3. Atribua usuários ao grupo.

Etapa 4: Compartilhe a URL da loja com seus usuários

Vá para **Citrix® StoreFront Cloud \> Acesso** e, em seguida, compartilhe o URL da loja com seus usuários.

Entregar PCs de escritório (não gerenciados por energia)

Esta seção o orienta pelo processo de implantação de entrega de PCs de escritório (não gerenciados por energia).

Pré-requisitos

Antes de começar, você precisa:

- Nomes das máquinas dos PCs.
- O Citrix Virtual Delivery Agent (VDA) está instalado em cada PC. (Esta etapa pode ser feita após a criação do catálogo.)

  Para obter mais informações, consulte Baixar VDA.

Preparação

Responda às perguntas na tela para concluir as seguintes configurações de nível de infraestrutura.

#	CONFIGURAÇÃO	DESCRIÇÃO
1	Selecione o tipo de alocação de máquina.	Selecione como as máquinas são atribuídas.
		Opções: Atribuição automática estática, pré-atribuição estática e pool aleatório não atribuído
2	Determine se os usuários podem ligar as máquinas	Mantenha **Quero que os usuários remotos liguem as máquinas por conta própria** desmarcado.
3	Selecione o tipo de identidade do usuário	Selecione um tipo de identidade para gerenciamento de usuários.

#	CONFIGURAÇÃO	DESCRIÇÃO
		Opções: Active Directory, Microsoft Entra ID, Google Cloud Identity e Okta

Etapas de implantação

Depois de concluir as configurações de nível de infraestrutura, as etapas específicas para este cenário de implantação aparecerão. Siga as instruções na tela para concluir as configurações.

Etapa 1: Adicionar um local de recurso

Configure seu local de recurso instalando os Cloud Connectors.

1. Nomeie o local de recurso.
2. Baixe e instale os Cloud Connectors em pelo menos duas máquinas Windows Server.
3. Detectar Cloud Connectors instalados.

> **Nota:**
>
> A criação de conexões de host é necessária apenas quando você deseja gerenciar o consumo de energia das máquinas.

Etapa 2: Criar um catálogo de Acesso Remoto para PC

Crie um catálogo e importe seus PCs de escritório para ele.

1. Nomeie o catálogo
2. Selecione um local de recurso.
3. Selecione um tipo de alocação. Por padrão, o tipo selecionado na fase de preparação é exibido.
4. Importe suas máquinas.
5. Clique em **Criar**.

Etapa 3: Criar grupos de entrega e atribuir usuários

Crie um grupo de entrega para as máquinas que você deseja entregar e especifique quem pode acessá-las.

1. Nomeie o grupo.
2. Selecione um catálogo de máquinas conforme necessário. Apenas os catálogos de **Acesso Remoto para PC** aparecem.
3. Atribua usuários para o grupo.

Etapa 4: Compartilhe a URL da loja com seus usuários

Vá para **Citrix® StoreFront Cloud \> Access** e, em seguida, compartilhe a URL da loja com seus usuários.

Identidades de máquina

Cada máquina deve ter uma identidade de máquina exclusiva, também conhecida como conta de computador. As identidades de máquina podem ser criadas e gerenciadas nas máquinas localmente ou em um diretório, como o Active Directory (AD) local ou o Microsoft Entra ID. A Citrix oferece suporte à hospedagem de aplicativos e desktops virtuais em máquinas que são ingressadas no Active Directory, ingressadas no Microsoft Entra, ingressadas no Microsoft Entra híbrido ou não ingressadas no domínio.

Tipos de identidade de máquina

Os seguintes tipos de identidade de máquina são suportados.

TIPO DE IDENTIDADE DE MÁQUINA	DESCRIÇÃO
Ingressado no AD	As identidades são criadas e gerenciadas no Active Directory local. As máquinas provisionadas são ingressadas no Active Directory local usando as identidades de máquina atribuídas.
Ingressado no Microsoft Entra	As identidades são criadas e gerenciadas no Entra ID. As máquinas provisionadas são ingressadas no Entra ID usando as identidades de máquina atribuídas. A importação de VMs para o Citrix DaaS não é suportada.
Ingressado no Microsoft Entra híbrido	As identidades são criadas no Active Directory local e são sincronizadas com o Entra ID por meio do Microsoft Entra Connect. As máquinas provisionadas são ingressadas no Active

TIPO DE IDENTIDADE DE MÁQUINA	DESCRIÇÃO
	Directory local e no Entra ID. As máquinas são então ingressadas no Entra híbrido. Para importar uma VM ingressada no Entra híbrido, a VM é tratada como uma VM ingressada no Active Directory pelo Citrix DaaS.
Não ingressado no domínio	As identidades são criadas e gerenciadas nas máquinas localmente. A importação de VMs para o Citrix DaaS não é suportada.

Configurações Suportadas

A seguir estão os detalhes das configurações suportadas para cada cenário.

Infraestrutura suportada

IDENTIDADE DA MÁQUINA	CITRIX DAAS™	CITRIX® STOREFRONT CLOUD	CITRIX STOREFRONT	CITRIX GATEWAY SERVICE	CITRIX GATEWAY
Unido ao AD	Sim	Sim	Sim	Sim	Sim
Unido ao Microsoft Entra	Sim	Sim	Pré-visualização	Sim	Não
Microsoft Entra híbrido associado	Sim	Sim	Sim	Sim	Sim
Não associado ao domínio	Sim	Sim	Sim	Sim	Sim

NOTA

Nem o Local Host Cache nem o Service Continuity estão disponíveis para hosts de sessão não associados ao domínio ao usar o Storefront.

Provedores de identidade de autenticação do Citrix® StoreFront Cloud suportados

IDENTIDADE DA MÁQUINA	MICROSOFT ENTRA ID	ACTIVE DIRECTORY	ACTIVE DIRECTORY E TOKEN	OKTA	SAML	CITRIX GATEWAY	AUTENTICAÇÃO ADAPTATIVA
Associado ao AD	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Microsoft Entra unido	Sim	Não	Não	Não	Sim	Não	Não
Microsoft Entra híbrido unido	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Não associado ao domínio	Sim	Sim	Sim	Sim	Sim	Sim	Sim

NOTA

- Se estiver usando um provedor de identidade diferente de Active Directory ou Active Directory + Token com implantações unidas ao AD ou unidas hibridamente ao Entra, você precisará do Citrix Federated Authentication Service (FAS) para obter logon único (SSO) para o aplicativo virtual ou sessão de desktop. Consulte a documentação do FAS para obter detalhes.

Se você planeja usar SAML como seu provedor de identidade e precisar de acesso a hosts de sessão unidos ao Microsoft Entra, consulte a documentação do Citrix Cloud para obter informações sobre como configurar SAML com identidades do Entra ID.

Active Directory associado

As identidades são criadas e gerenciadas no Active Directory local. As máquinas provisionadas são associadas ao Active Directory local usando as identidades de máquina atribuídas. Para obter mais informações sobre os níveis funcionais suportados para a floresta e o domínio, consulte Níveis funcionais do Active Directory.

Para obter informações sobre como criar um pool de identidades de máquina associadas ao Active Directory (AD) local usando o Citrix DaaS, consulte Pool de identidades de máquina associadas ao Active Directory local.

Microsoft Entra ingressado

Este artigo descreve os requisitos para criar catálogos ingressados no Microsoft Entra usando o Citrix DaaS™, além dos requisitos descritos na seção de requisitos do sistema do Citrix DaaS.

Requisitos

- Plano de controle: Consulte Configurações Suportadas
- Tipo de VDA: Sessão única (somente desktops) ou multi-sessão (aplicativos e desktops)
- Versão do VDA: 2203 ou posterior
- Tipo de provisionamento: Machine Creation Services™ (MCS), Persistente e Não persistente usando o fluxo de trabalho de Perfil de Máquina
- Tipo de atribuição: Dedicado e agrupado
- Plataforma de hospedagem: Somente Azure
- O Rendezvous V2 deve estar habilitado
- Logon único: Consulte Logon único do Microsoft Entra para DaaS

Limitações

- A continuidade do serviço não é suportada.
- O logon com o Windows Hello no desktop virtual é suportado apenas com PIN. Métodos de autenticação biométrica (reconhecimento facial, reconhecimento de impressão digital e reconhecimento de íris) não são suportados no momento.
- Suporta apenas ambientes de nuvem do Microsoft Azure Resource Manager.
- Se o logon único estiver desabilitado, na primeira vez que uma sessão de área de trabalho virtual for iniciada, a tela de logon do Windows poderá mostrar o prompt de logon para o último usuário conectado sem a opção de alternar para outro usuário. O usuário deve esperar até

que o logon expire e a tela de bloqueio da área de trabalho apareça, e então clicar na tela de bloqueio para revelar a tela de logon novamente. Neste ponto, o usuário pode selecionar **Outros Usuários** e inserir suas credenciais. Este é o comportamento em cada nova sessão quando as máquinas são não persistentes.

- Quando vários catálogos de máquinas são unidos ao mesmo locatário do Azure, cada catálogo deve usar um `NamingScheme` exclusivo. Se catálogos diferentes usarem o mesmo `NamingScheme`, as VMs podem ser criadas com nomes duplicados, o que faz com que a união do Entra ID falhe devido a conflitos de nomes.

Considerações

Configuração da imagem

- Considere otimizar sua imagem do Windows usando a ferramenta Citrix Optimizer.

Unido ao Microsoft Entra

- Considere desabilitar o Windows Hello para que os usuários não sejam solicitados a configurá-lo ao fazer login em sua área de trabalho virtual. Se você estiver usando o VDA 2209 ou posterior, isso é feito automaticamente. Para versões anteriores, você pode fazer isso de uma das duas maneiras:
    - Política de grupo ou política local
        - navegar até **Configuração do Computador > Modelos Administrativos > Componentes do Windows > Windows Hello para Empresas**.
        - Defina **Usar Windows Hello para Empresas** como:
            - **Desabilitado**, ou
            - **Habilitado** e selecione **Não iniciar o provisionamento do Windows Hello após o logon**.
    - Microsoft Intune
        - Crie um perfil de dispositivo que desabilite o Windows Hello para Empresas. Consulte a documentação da Microsoft para obter detalhes.
- Os usuários devem ter acesso explícito concedido no Azure para fazer login nas máquinas usando suas credenciais do Microsoft Entra. Isso pode ser facilitado adicionando a atribuição de função no nível do grupo de recursos:

    a. Faça login no portal do Azure.

b. Selecione **Grupos de recursos**.

c. Clique no grupo de recursos onde as cargas de trabalho da área de trabalho virtual residem.

d. Selecione **Controle de acesso (IAM)**.

e. Clique em **Adicionar atribuição de função**.

f. Procure por **Virtual Machine User Login**, selecione-o na lista e clique em **Avançar**.

g. Selecione **Usuário, grupo ou entidade de serviço**.

h. Clique em **Selecionar membros** e selecione os usuários e grupos aos quais você deseja fornecer acesso às áreas de trabalho virtuais.

i. Clique em **Selecionar**.

j. Clique em **Revisar + atribuir**.

k. Clique em **Revisar + atribuir** novamente.

> **Nota:**
>
> Se você optar por permitir que o MCS crie o grupo de recursos para as áreas de trabalho virtuais, adicione esta atribuição de função após a criação do catálogo de máquinas.

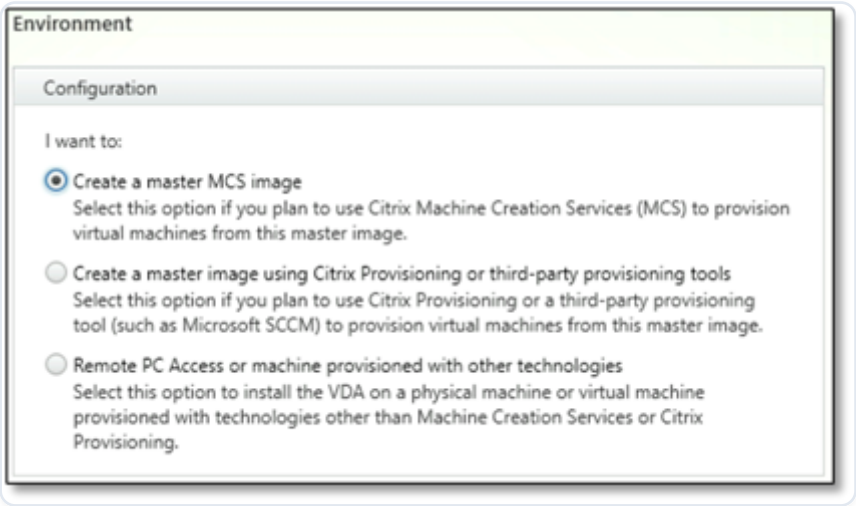
- As VMs mestre podem ser ingressadas no Microsoft Entra ou não ingressadas no domínio. Essa funcionalidade requer a versão 2212 ou posterior do VDA.

Instalação e configuração do VDA

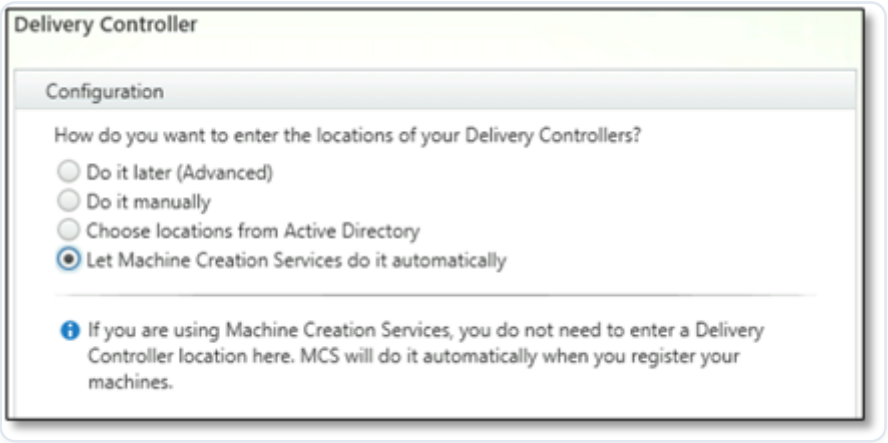
Siga as etapas para instalar o VDA:

1. Certifique-se de selecionar as seguintes opções no assistente de instalação:

    - Na página Ambiente, selecione **Criar uma imagem mestre MCS**.



- Na página Delivery Controller™, selecione **Deixar o Machine Creation Services fazer isso automaticamente**.



2. (Somente para versões do VDA anteriores a 2311) Após a instalação do VDA, adicione o seguinte valor de registro:

   - Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Tipo de valor: DWORD
   - Nome do valor: GctRegistration
   - Dados do valor: 1

3. Para uma VM mestre baseada no Windows 11 22H2, crie uma tarefa agendada na VM mestre que execute o seguinte comando na inicialização do sistema usando a conta SYSTEM. Esta tarefa de agendamento de uma tarefa na VM mestre é necessária apenas para a versão 2212 ou anterior do VDA.

   ```
   reg ADD HKLM\Software\AzureAD\VirtualDesktop /v Provider /t REG_SZ /d Citrix /f
   ```

4. Se você unir a VM mestre ao Microsoft Entra ID e, em seguida, remover manualmente a união usando o utilitário `dsregcmd`, certifique-se de que o valor de `AADLoginForWindowsExtensionJoined` em HKLM\Software\Microsoft\Windows Azure\CurrentVersion\AADLoginForWindowsExtension seja zero.

Onde ir em seguida

Uma vez que o local do recurso e a conexão de hospedagem estejam disponíveis, prossiga para criar o catálogo de máquinas. Para obter mais informações sobre como criar um pool de identidades de máquina unida ao Microsoft Entra, consulte Pool de identidades de máquina unida ao Microsoft Entra.

Microsoft Intune

Este artigo descreve os requisitos para criar catálogos habilitados para Microsoft Intune usando o Citrix DaaS™ além dos requisitos descritos na seção de requisitos de sistema do Citrix DaaS.

Microsoft Intune é um serviço baseado em nuvem que se concentra no gerenciamento de dispositivos móveis (MDM) e no gerenciamento de aplicativos móveis (MAM). Você controla como os dispositivos da sua organização são usados, incluindo telefones celulares, tablets e laptops. Para obter mais informações, consulte Microsoft Intune. Os dispositivos devem atender aos requisitos mínimos do sistema. Para obter mais informações, consulte a documentação da Microsoft Sistemas operacionais e navegadores compatíveis no Intune.

> **Importante:**

> Antes de habilitar este recurso, verifique se seu ambiente Azure atende aos requisitos de licenciamento para usar o Microsoft Intune. Para obter mais informações, consulte a documentação da Microsoft: `<https://docs.microsoft.com/pt-br/mem/intune/fundamentals/licenses>`. Não habilite o recurso se você não tiver a licença Intune apropriada.

> Você pode criar:

- Catálogos unidos ao Microsoft Entra registrados no Microsoft Intune para VMs persistentes e não persistentes, de sessão única e multi-sessão. Para requisitos, limitações e considerações, consulte Requisitos para catálogos unidos ao Microsoft Entra registrados no Microsoft Intune.
- Catálogos híbridos unidos ao Microsoft Entra registrados no Microsoft Intune para VMs persistentes de sessão única e multi-sessão usando credencial de dispositivo com capacidade

de co-gerenciamento. Para requisitos, limitações e considerações, consulte Requisitos para catálogos híbridos unidos ao Microsoft Entra registrados no Microsoft Intune. Você também pode criar catálogos híbridos unidos ao Microsoft Entra registrados no Microsoft Intune para VMs não persistentes de sessão única e multi-sessão. No entanto, isso está atualmente em Pré-visualização. Consulte Registro de VMs não persistentes unidas ao Hybrid Entra ID no Microsoft Intune.

Requisitos para catálogos unidos ao Microsoft Entra registrados no Microsoft Intune

- Plano de controle: Citrix DaaS
- Tipo de VDA: VDA de SO de sessão única e multi-sessão
- Versão do VDA

TIPO DE CATÁLOGO	VERSÃO DO VDA
Catálogos unidos ao Microsoft Entra registrados no Microsoft Intune para VMs persistentes, de sessão única e multi-sessão	2203 e posterior
Catálogos unidos ao Microsoft Entra inscritos no Microsoft Intune para VMs não persistentes, de sessão única e de múltiplas sessões	2407 e posterior

- Tipo de provisionamento: Catálogos de máquinas persistentes e não persistentes do Machine Creation Services™ (MCS) usando apenas o fluxo de trabalho de Perfil de Máquina

Limitações para catálogos unidos ao Microsoft Entra inscritos no Microsoft Intune

- Não pule a preparação da imagem ao criar ou atualizar catálogos de máquinas.

Considerações para catálogos unidos ao Microsoft Entra inscritos no Microsoft Intune

- Crie um perfil de dispositivo que desabilite o Windows Hello for Business.
- Use a versão 2212 ou posterior do VDA se o Microsoft Intune precisar gerenciar uma VM mestre.

- Configure o Microsoft Intune para excluir os dispositivos obsoletos. Isso garante que seus registros de dispositivo permaneçam atualizados. Para obter informações sobre como excluir dispositivos obsoletos, consulte Excluir dispositivos automaticamente com regras de limpeza.

Catálogos híbridos unidos ao Microsoft Entra inscritos no Microsoft Intune

Catálogos híbridos unidos ao Microsoft Entra, VMs persistentes de sessão única e de múltiplas sessões, inscritos no Microsoft Intune usam as credenciais do dispositivo com capacidade de cogestão.

A cogestão permite gerenciar simultaneamente dispositivos Windows 10 ou posteriores usando o Configuration Manager e o Microsoft Intune. Para obter mais informações, consulte Cogestão.

Pré-requisitos para catálogos híbridos unidos ao Microsoft Entra inscritos no Microsoft Intune

Antes de habilitar este recurso, verifique se:

- Seu ambiente Azure atende aos requisitos de licenciamento para usar o Microsoft Intune. Para mais informações, consulte a documentação da Microsoft.
- Você tem uma implantação válida do Configuration Manager com co-gerenciamento habilitado. Para mais informações, consulte a documentação da Microsoft.

Requisitos para catálogos híbridos do Microsoft Entra ingressados e registrados no Microsoft Intune

- Plano de controle: Citrix DaaS
- Tipo de VDA: Sessão única ou multi-sessão
- Versão do VDA: 2407 ou posterior
- Tipo de provisionamento: Machine Creation Service (MCS), Persistente
- Tipo de atribuição: Dedicado e agrupado
- Plataforma de hospedagem: Qualquer hipervisor ou serviço de nuvem

Limitações para catálogos híbridos do Microsoft Entra ingressados e registrados no Microsoft Intune

- Não pule a preparação da imagem ao criar ou atualizar catálogos de máquinas.
- O gerenciamento de cliente baseado na Internet (IBCM) do Configuration Manager não é suportado.

Considerações para catálogos híbridos do Microsoft Entra ingressados e registrados no Microsoft Intune

- O registro no Intune pode ser atrasado se muitas máquinas no catálogo forem ligadas simultaneamente.

  A Microsoft impõe uma restrição de registro no Intune por locatário que limita o número de dispositivos que podem ser registrados dentro de um período específico. O número permitido de dispositivos varia dependendo do número de licenças do Microsoft Intune associadas ao locatário. Consulte sua equipe de contas da Microsoft para descobrir o limite permitido para seu locatário. Essa abordagem ajuda o registro do Microsoft Intune a escalar melhor para grandes ambientes.

  Para máquinas persistentes, pode haver um tempo de espera inicial necessário para que todos os dispositivos concluam o registro no Intune.

- Configure o Cloud Attach do Configuration Manager. Para obter mais informações, consulte a documentação da Microsoft.
- Instale manualmente o cliente do Configuration Manager na VM mestre sem atribuir o código do site com `.\CCMSetup.exe /mp:SCCMServer /logon FSP=SCCMServer`. O SCCMServer é o nome do servidor SCCM em seu ambiente. Para obter mais informações, consulte a documentação da Microsoft.
- As máquinas criadas pelo MCS usam o mecanismo de atribuição automática de site para encontrar grupos de limites de site que são publicados nos Serviços de Domínio do Active Directory. Certifique-se de que os limites e grupos de limites do **Configuration Manager** estejam configurados em seu ambiente. Se a atribuição automática de site não estiver disponível, um código de site estático do Configuration Manager pode ser configurado na VM mestre por meio da seguinte configuração de registro:

  Chave:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MachineIdentityServiceAgent\DeviceMa
  nagement
  ```

  Nome do valor: `MdmSccmSiteCode`

  Tipo de valor: **String**

  Dados do valor: `the site code to be assigned`

- Configure o Microsoft Intune para excluir os dispositivos obsoletos. Isso garante que seus registros de dispositivo permaneçam atualizados. Para obter informações sobre como excluir dispositivos obsoletos, consulte Excluir dispositivos automaticamente com regras de limpeza.

Onde ir em seguida

- Para obter informações sobre como criar um pool de identidades de máquina habilitadas para Microsoft Intune, consulte Pool de identidades de máquina habilitadas para Microsoft Intune.

Microsoft Entra híbrido associado

Este artigo descreve os requisitos para criar catálogos híbridos associados ao Microsoft Entra usando o Citrix DaaS, além dos requisitos descritos na seção de requisitos do sistema do Citrix DaaS.

Este artigo descreve os requisitos para criar catálogos associados ao Hybrid Azure Active Directory (HAAD) usando o Citrix DaaS™, além dos requisitos descritos na seção de requisitos do sistema do Citrix DaaS.

Máquinas associadas ao Azure AD híbrido usam o AD local como provedor de autenticação. Você pode atribuí-las a usuários ou grupos de domínio no AD local. Para habilitar a experiência de SSO contínuo do Azure AD, você precisa ter os usuários de domínio sincronizados com o Azure AD.

> **Nota:**
>
> VMs associadas ao Microsoft Entra híbrido são suportadas em infraestruturas de identidade federadas e gerenciadas.

Requisitos

- Plano de controle: Consulte Configurações Suportadas
- Tipo de VDA: Sessão única (somente desktops) ou multissessão (aplicativos e desktops)
- Versão do VDA: 2212 ou posterior
- Tipo de provisionamento: Machine Creation Services™ (MCS), Persistente e Não persistente
- Tipo de atribuição: Dedicado e agrupado
- Plataforma de hospedagem: Qualquer hipervisor ou serviço de nuvem

Limitações

- Se o Citrix Federated Authentication Service (FAS) for usado, o logon único será direcionado ao AD local em vez do Microsoft Entra ID. Nesse caso, é recomendável configurar a autenticação baseada em certificado do Microsoft Entra para que o token de atualização primário (PRT) seja gerado no logon do usuário, o que facilita o logon único em recursos do Microsoft Entra dentro da sessão. Caso contrário, o PRT não estará presente e o SSO para recursos do Microsoft Entra não funcionará. Para obter informações sobre como obter o logon único (SSO) do Microsoft Entra para VDAs associados a híbridos usando o Citrix Federated Authentication Service (FAS), consulte VDAs associados a híbridos.
- Não pule a preparação da imagem ao criar ou atualizar catálogos de máquinas. Se você quiser pular a preparação da imagem, certifique-se de que as VMs mestras não sejam ingressadas no Microsoft Entra ou no Microsoft Entra híbrido.

Considerações

- A criação de máquinas ingressadas no Microsoft Entra híbrido requer a permissão `Write userCertificate` no domínio de destino. Certifique-se de inserir as credenciais de um administrador com essa permissão durante a criação do catálogo.
- O processo de ingresso híbrido no Microsoft Entra é gerenciado pela Citrix. Você precisa desabilitar `autoWorkplaceJoin` controlado pelo Windows nas VMs mestras da seguinte forma. A tarefa de desabilitar manualmente `autoWorkplaceJoin` é necessária apenas para a versão 2212 ou anterior do VDA.

  a. Execute `gpedit.msc`.

  b. navegar até **Configuração do Computador > Modelos Administrativos > Componentes do Windows > Registro de Dispositivo**.

  c. Defina **Registrar computadores ingressados no domínio como dispositivos** como **Desabilitado**.

- Selecione a Unidade Organizacional (OU) que está configurada para ser sincronizada com o Microsoft Entra ID ao criar as identidades da máquina.
- Para VM mestra baseada no Windows 11 22H2, crie uma tarefa agendada na VM mestra que executa os seguintes comandos na inicialização do sistema usando a conta SYSTEM. Esta tarefa de agendamento de uma tarefa na VM mestra é necessária apenas para a versão 2212 ou anterior do VDA.

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'

$WorkplaceJoinKeyPath = 'HKLM:
\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin'

$MaxCount = 60



for ($count = 1; $count -le $MaxCount; $count++)

{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)

  {

    $provider = (Get-Item -Path
$VirtualDesktopKeyPath).GetValue("Provider", $null)

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "Provider"
-Value "Citrix" -Force

        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name
"autoWorkplaceJoin" -Value 1 -Force

        Start-Sleep 5

        dsregcmd /join
```

```
        break
    }
  }

  Start-Sleep 1
}
```

- Por padrão, o Microsoft Entra Connect sincroniza a cada 30 minutos. As máquinas provisionadas podem levar até 30 minutos para serem ingressadas no Microsoft Entra híbrido durante a primeira inicialização.

Onde ir em seguida

Para obter mais informações sobre como criar um pool de identidades de máquina ingressada no Microsoft Entra híbrido, consulte Pool de identidades de máquina ingressada no Microsoft Entra híbrido.

Não associado a domínio

Este artigo descreve os requisitos para criar catálogos não associados a domínio usando o Citrix DaaS™, além dos requisitos descritos na seção de requisitos de sistema do Citrix DaaS.

Requisitos

- Plano de controle: Consulte Configurações Suportadas
- Tipo de VDA: Sessão única (somente desktops) ou multi-sessão (aplicativos e desktops)
- Versão do VDA: 2203 ou posterior
- Tipo de provisionamento: Machine Creation Services™ (MCS), Persistente e Não persistente
- Tipo de atribuição: Dedicado e agrupado
- Plataforma de hospedagem: Todas as plataformas suportadas pelo MCS
- O Rendezvous V2 deve estar ativado
- Cloud Connectors: Necessário apenas se você planeja provisionar máquinas em hipervisores locais ou se deseja usar o Active Directory como provedor de identidade no Workspace.

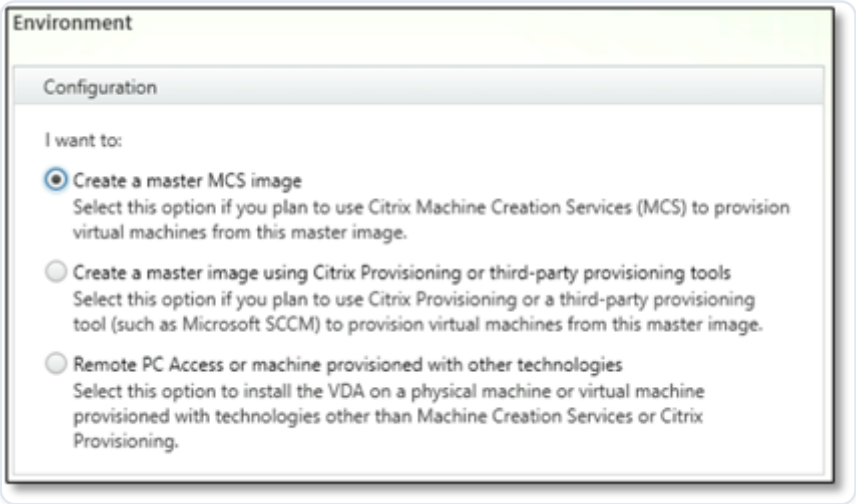
Limitações

- A continuidade do serviço não é suportada.
- Sempre que usamos um VDA multi-sessão não associado a domínio, os dados de perfil do usuário local não são retidos e são excluídos no logoff.

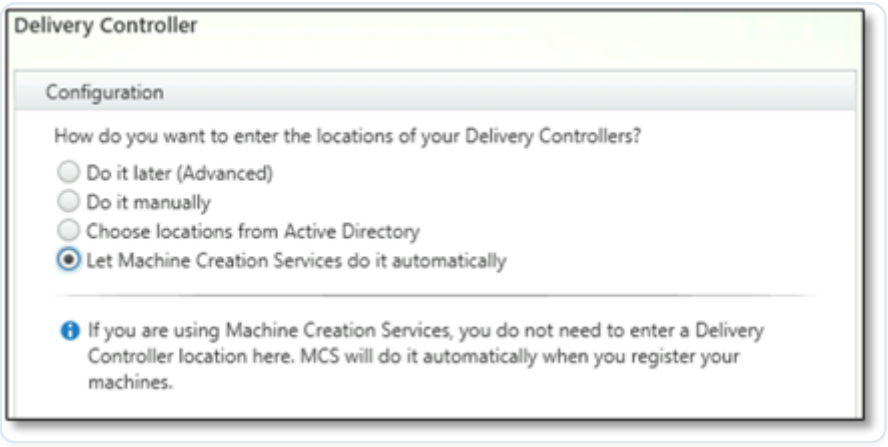
Instalação e configuração do VDA

Siga os passos para instalar o VDA:

1. Certifique-se de selecionar as seguintes opções no assistente de instalação:
    - Na página Ambiente, selecione **Criar uma imagem mestre MCS**.



    - Na página Delivery Controller™, selecione **Deixar que o Machine Creation Services faça isso automaticamente**.



2. Após a instalação do VDA, adicione o seguinte valor de registro:
    - Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
    - Tipo de valor: DWORD

- Nome do valor: GctRegistration
- Dados do valor: 1

Onde ir a seguir

Uma vez que o local do recurso e a conexão de hospedagem estejam disponíveis, prossiga para criar o catálogo de máquinas. Para mais informações sobre a criação de pool de identidades de máquinas não associadas ao domínio, consulte Pool de identidades de máquinas não associadas ao domínio.

Autenticação de sessão

O Citrix oferece suporte a vários métodos para autenticar usuários em sessões de desktop virtual e aplicativo. As opções disponíveis dependem de como seu ambiente está configurado; especificamente, o serviço de diretório onde as contas de usuário residem (por exemplo, Active Directory ou Microsoft Entra ID), o serviço de diretório ao qual as máquinas host de sessão estão unidas e o provedor de identidade usado para o logon inicial no ambiente Citrix. Esses fatores determinam se a autenticação pode ser tratada por meio de credenciais tradicionais, cartões inteligentes, asserções federadas ou mecanismos baseados em certificado. Esta seção descreve os métodos de autenticação disponíveis e como eles se alinham com diferentes cenários de implantação.

Logon único do Microsoft Entra

Você pode aproveitar o logon único (SSO) ao usar credenciais do Microsoft Entra ID para acessar aplicativos e desktops virtuais em hosts de sessão ingressados no Microsoft Entra ou ingressados no Microsoft Entra híbrido.

Infraestrutura suportada

A seguir, uma visão geral dos componentes de infraestrutura suportados para o logon único do Microsoft Entra:

IDENTIDADE DA MÁQUINA	CITRIX DAAS	CITRIX DAAS LOCAL	CITRIX STOREFRONT CLOUD	CITRIX STOREFRONT	CITRIX GATEWAY SERVICE	NETSCALER GATEWAY
Ingressado no	Sim	Não	Sim	Não	Sim	Sim

IDENTIDADE DA MÁQUINA	CITRIX DAAS	CITRIX DAAS LOCAL	CITRIX STOREFRONT CLOUD	CITRIX STOREFRONT	CITRIX GATEWAY SERVICE	NETSCALER GATEWAY
Microsoft Entra						
Microsoft Entra híbrido ingressado	Sim	Sim	Sim	Sim	Sim	Sim

NOTA:

- Para obter detalhes sobre a configuração do logon único do Microsoft Entra com o **Citrix DaaS Local**, consulte a documentação do Citrix DaaS Local.
- Para obter detalhes sobre a configuração do logon único do Microsoft Entra com o **StoreFront**, consulte a documentação do StoreFront.

Provedores de identidade compatíveis

A seguir, uma visão geral dos provedores de identidade do Workspace compatíveis com o logon único do Microsoft Entra:

IDENTIDADE DA MÁQUINA	ENTRA ID	ACTIVE DIRECTORY	ACTIVE DIRECTORY + TOKEN	OKTA	SAML	NETSCALER GATEWAY	AUTENTICAÇÃO ADAPTATIVA
Ingressado no Microsoft Entra	Sim	Não	Não	Não	Sim	Não	Não
Microsoft Entra híbrido	Sim	Não	Não	Não	Sim	Não	Não

CITRIX DAAS™

IDENTIDADE DA MÁQUINA	ENTRA ID	ACTIVE DIRECTORY	ACTIVE DIRECTORY + TOKEN	OKTA	SAML	NETSCALER GATEWAY	AUTENTICAÇÃO ADAPTATIVA
ingressado							

NOTA

Se você planeja usar SAML como seu IdP, você deve garantir que seu provedor SAML esteja configurado corretamente para oferecer suporte à autenticação baseada em Entra. Consulte SAML usando Microsoft Entra ID e identidades Microsoft Entra para autenticação de espaço de trabalho.

Métodos de acesso suportados

A seguir estão os métodos de acesso disponíveis em um ambiente Citrix:

- **Acesso nativo:** Você usa o cliente nativo do aplicativo Citrix Workspace para acessar sua loja e estabelecer a conexão da sessão.
- **Acesso via navegador:** Você acessa sua loja por meio de um navegador e se conecta ao aplicativo virtual ou à sessão da área de trabalho usando o cliente Citrix Workspace app para HTML5.
- **Acesso híbrido:** Você acessa sua loja por meio de um navegador e se conecta ao aplicativo virtual ou à sessão de desktop usando o cliente nativo do aplicativo Workspace.

A seguir, uma visão geral dos métodos de acesso suportados para o logon único do Microsoft Entra:

MÉTODO DE ACESSO	WINDOWS	LINUX	MAC	CHROME OS	ANDROID	IOS
Nativo	Sim	Sim	Sim	Sim	Sim	Sim
Navegador	Sim	Sim	Sim	Sim	Sim	Sim

MÉTODO DE ACESSO	WINDOWS	LINUX	MAC	CHROME OS	ANDROID	IOS
Híbrido	Sim	Sim	Sim	Não	Não	Não

Requisitos do sistema

A seguir estão os requisitos do sistema para usar o logon único do Microsoft Entra:

- Plano de controle: Citrix DaaS
  - Citrix Cloud Commercial (EUA, UE e APS)
  - Citrix Cloud Japan
- Portal do usuário: Citrix® StoreFront Cloud
- Virtual Delivery Agent (VDA)
  - Windows: versão 2507 ou mais recente
- Aplicativo Citrix Workspace
  - Windows: versão 2507 ou mais recente
  - Linux: versão 2508 ou mais recente (versão 2601 ou mais recente necessária para acesso híbrido)
  - Mac: versão 2508 ou mais recente (versão 2511 ou mais recente necessária para acesso híbrido)
  - HTML5: versão 2511 ou mais recente
  - Chrome OS: versão 2511 ou mais recente
  - Android: versão 2511 ou mais recente
  - iOS: versão 2511 ou mais recente
- Extensão Web Citrix
  - Microsoft Edge
  - Google Chrome
- SO do host de sessão:
  - Windows 11, versão 24H2 com Atualizações Cumulativas de 2025-09 para Windows 11 (KB5065789) ou posterior instalado (compilação 26100.6725)

- Windows Server 2025 com Atualizações Cumulativas de 2026-01 para Windows Server 2025 (KB5073379) ou posterior instalado (compilação 26100.32230)

NOTA

A Extensão Web Citrix só é necessária se os seus usuários estiverem utilizando acesso híbrido em dispositivos **Windows**, **Linux** ou **Mac**. Se os seus usuários utilizarem acesso nativo ou via navegador, a Extensão Web Citrix não é necessária.

Considerações

- Se os seus usuários estiverem utilizando acesso híbrido, eles devem usar o Microsoft Edge ou o Google Chrome e instalar a Extensão Web Citrix. O logon único do Microsoft Entra com acesso híbrido não é compatível com outros navegadores.
- O Reconexão Automática do Cliente não é compatível quando o logon único do Microsoft Entra é usado para fazer logon na sessão. Este recurso é automaticamente desativado quando este método de logon é utilizado. A Confiabilidade da Sessão ainda está disponível para reconexão automática em caso de interrupções de rede.
- Quando um desktop virtual é bloqueado, o comportamento padrão é exibir a tela de bloqueio do Windows. Dependendo dos seus requisitos de autenticação, você pode precisar alterar o comportamento de bloqueio da sessão. Consulte Comportamento de bloqueio da sessão para mais detalhes.
- Se estiver usando hosts de sessão híbridos do Microsoft Entra, o logon único não funciona por padrão para membros de grupos privilegiados, como Administradores de Domínio. Para habilitá-lo, adicione o grupo ou usuário à lista de permissões do Controlador de Domínio Somente Leitura (RODC) para acesso ao Microsoft Entra Kerberos. Consulte TGT do Microsoft Entra Kerberos e controle de acesso do Active Directory para obter detalhes.
- O Microsoft Entra External ID não é compatível no momento. Se você precisar fornecer acesso a usuários convidados, consulte SAML usando Entra ID para identidades de convidado e B2B para autenticação de workspace.
- O logon único do Microsoft Entra exige que a configuração do Windows **Permitir que SSPs e APs personalizados sejam carregados no LSASS** esteja habilitada (padrão). Observe que, se você implantar o modelo **Linha de Base de Segurança para Windows 10 e posterior** via Microsoft Intune, essa configuração será desabilitada automaticamente e bloqueará o SSO, portanto, você deve atualizar sua política de configuração de dispositivo do Intune para mantê-la habilitada.

Como configurar o logon único do Microsoft Entra

Visão geral

A configuração do logon único do Microsoft Entra consiste nas seguintes etapas:

1. Configuração do Azure e do Microsoft Entra ID
    a. Registrar os aplicativos cliente e de recurso Citrix.
    b. Habilitar o protocolo de autenticação dos Serviços de Área de Trabalho Remota do Microsoft Entra ID para o aplicativo de recurso Citrix.
    c. Ocultar o prompt de consentimento do usuário.
    d. Aprovar o aplicativo cliente.
    e. Criar um objeto de servidor Kerberos (somente ambientes híbridos do Microsoft Entra).
    f. Revisar as políticas de Acesso Condicional do Microsoft Entra.
2. Configuração do Citrix
    a. Provisionar hosts de sessão com a versão de SO, tipo de identidade e versão de VDA necessários.
    b. Configurar o Citrix® StoreFront Cloud:
        i. Configurar um Provedor de Identidade apropriado.
        ii. Habilitar logon único do Microsoft Entra
    c. Configurar o tipo de logon dos seus Delivery Groups se necessário.

Os detalhes de cada etapa de configuração são fornecidos nas seções a seguir.

Configuração do Azure e do Microsoft Entra ID

Para aproveitar o logon único do Microsoft Entra, você deve primeiro permitir a autenticação do Microsoft Entra para Windows em seu locatário do Microsoft Entra ID, o que permite a emissão dos tokens de autenticação necessários que permitem aos usuários fazer logon nos hosts de sessão ingressados no Microsoft Entra e ingressados no Microsoft Entra híbrido.

A pessoa que realiza a configuração do Azure deve ter uma das seguintes funções internas do Microsoft Entra ou equivalente, no mínimo:

- Administrador de Aplicativos
- Administrador de Aplicativos na Nuvem

A configuração pode ser concluída através do Portal do Azure, usando o SDK do Microsoft Graph PowerShell ou a API do Microsoft Graph. As seções a seguir fornecem detalhes para concluir a configuração através do Portal do Azure. Se você preferir usar o SDK do Microsoft Graph PowerShell ou a API do Microsoft Graph, consulte configuração do Azure para logon único do Microsoft Entra.

REGISTRAR APLICATIVOS CITRIX

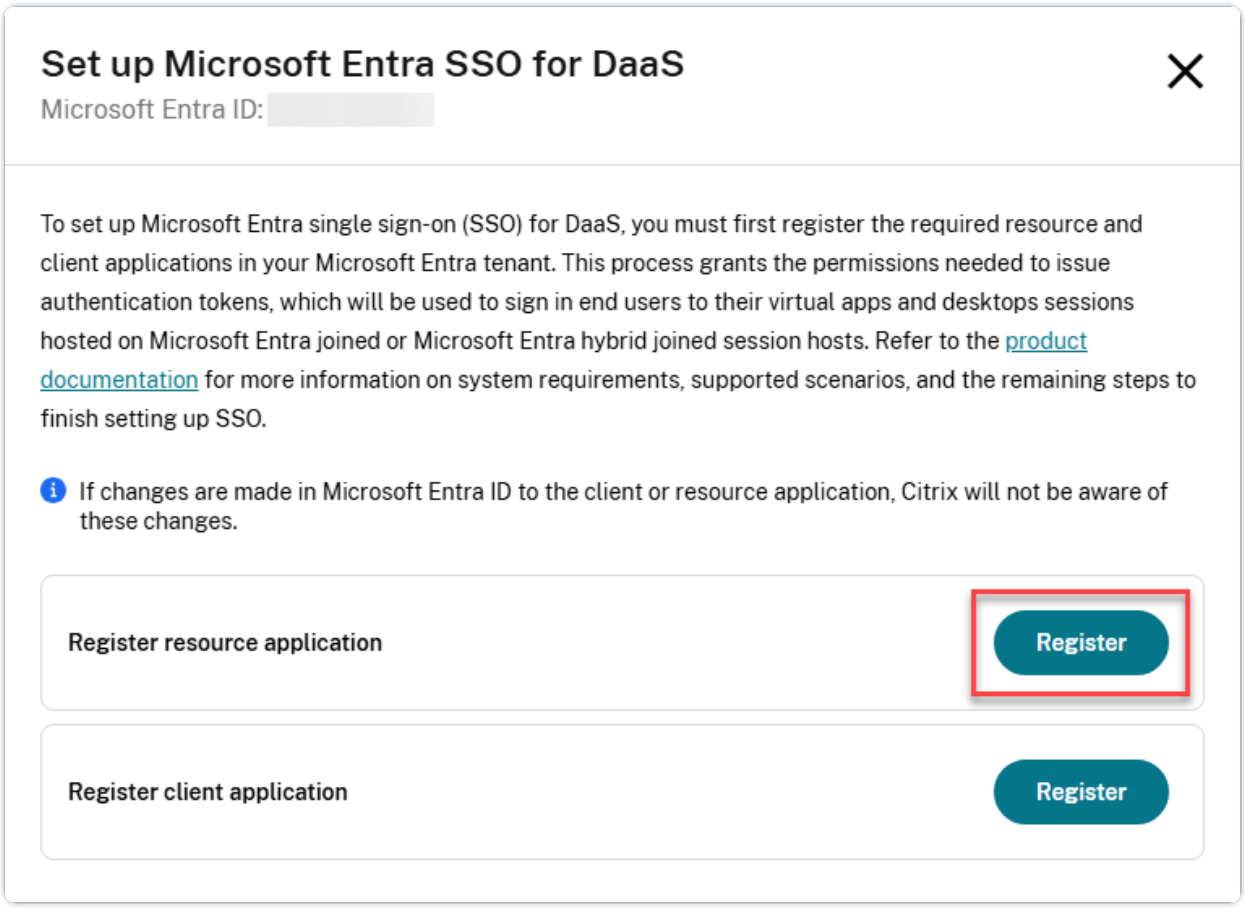
O logon único do Microsoft Entra requer um Aplicativo de Recurso do Entra ID e um Aplicativo Cliente do Entra ID. O Aplicativo de Recurso representa o sistema operacional Windows ao solicitar o Token de Acesso RDP. O Aplicativo Cliente representa o aplicativo Citrix Workspace.

Você pode registrar os aplicativos de Recurso Citrix e Cliente Citrix através do **portal Citrix Cloud**:

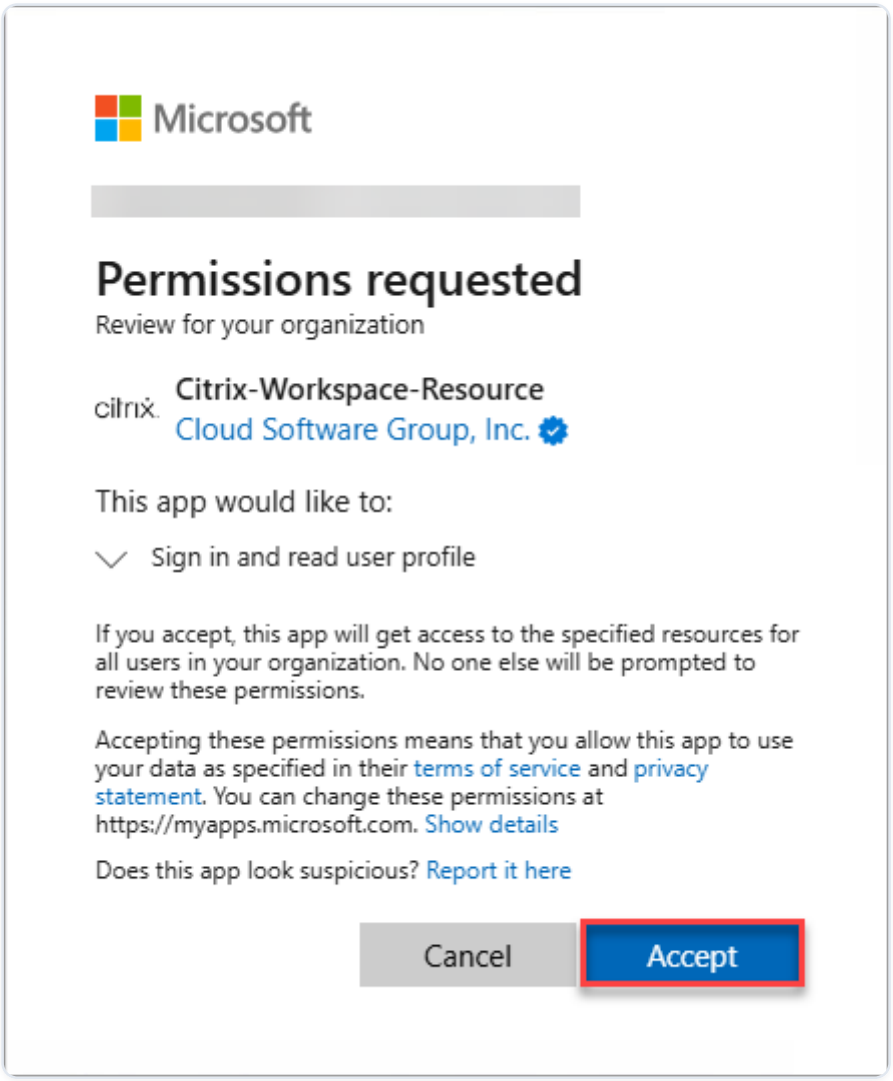
1. Abra o menu no canto superior esquerdo e selecione `Identity and access management`.
2. Na página `Authentication`, procure o provedor de identidade do Microsoft Entra ID para o qual você deseja habilitar o logon único do Microsoft Entra.
3. Abra o menu de opções e selecione `Set up Microsoft Entra SSO`.



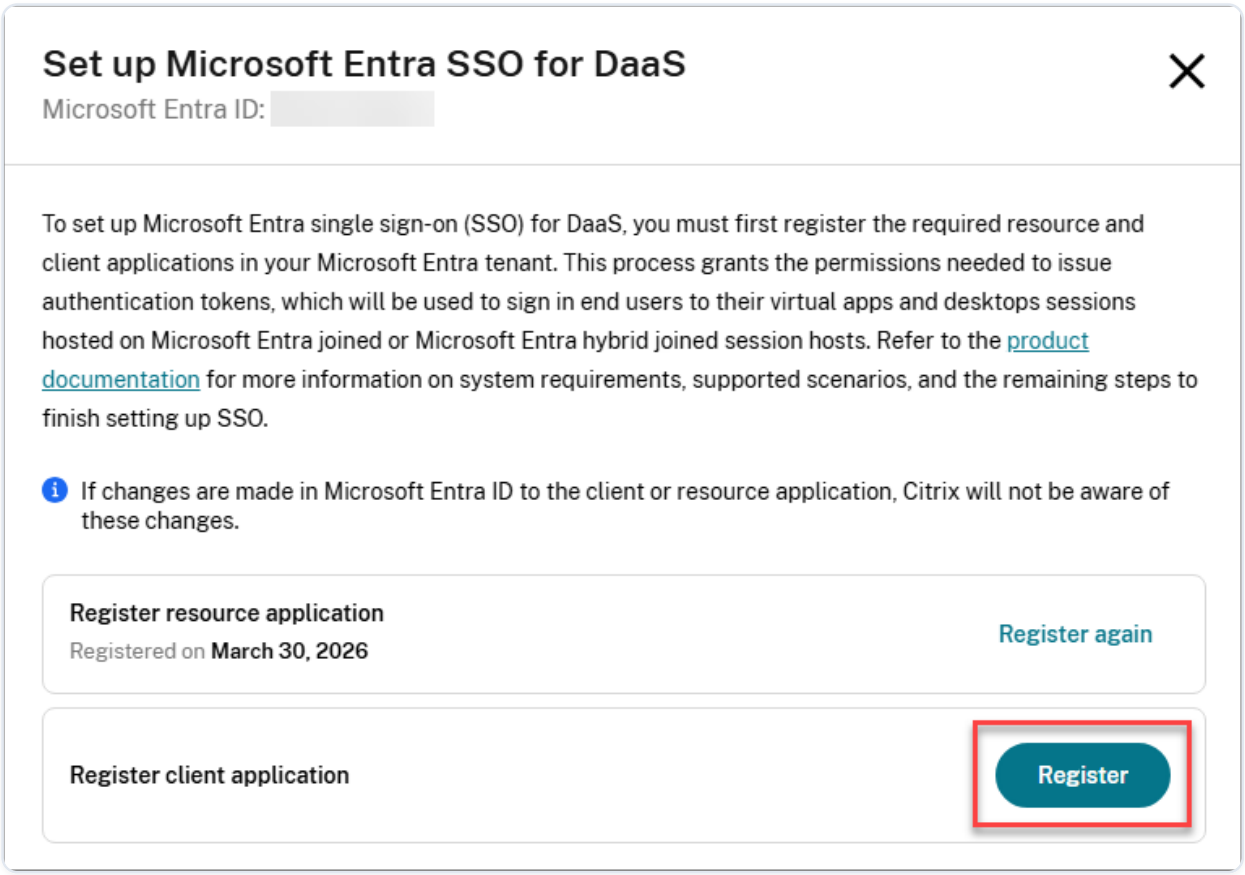
4. Clique em `Register` ao lado de **Registrar aplicativo de recurso**.



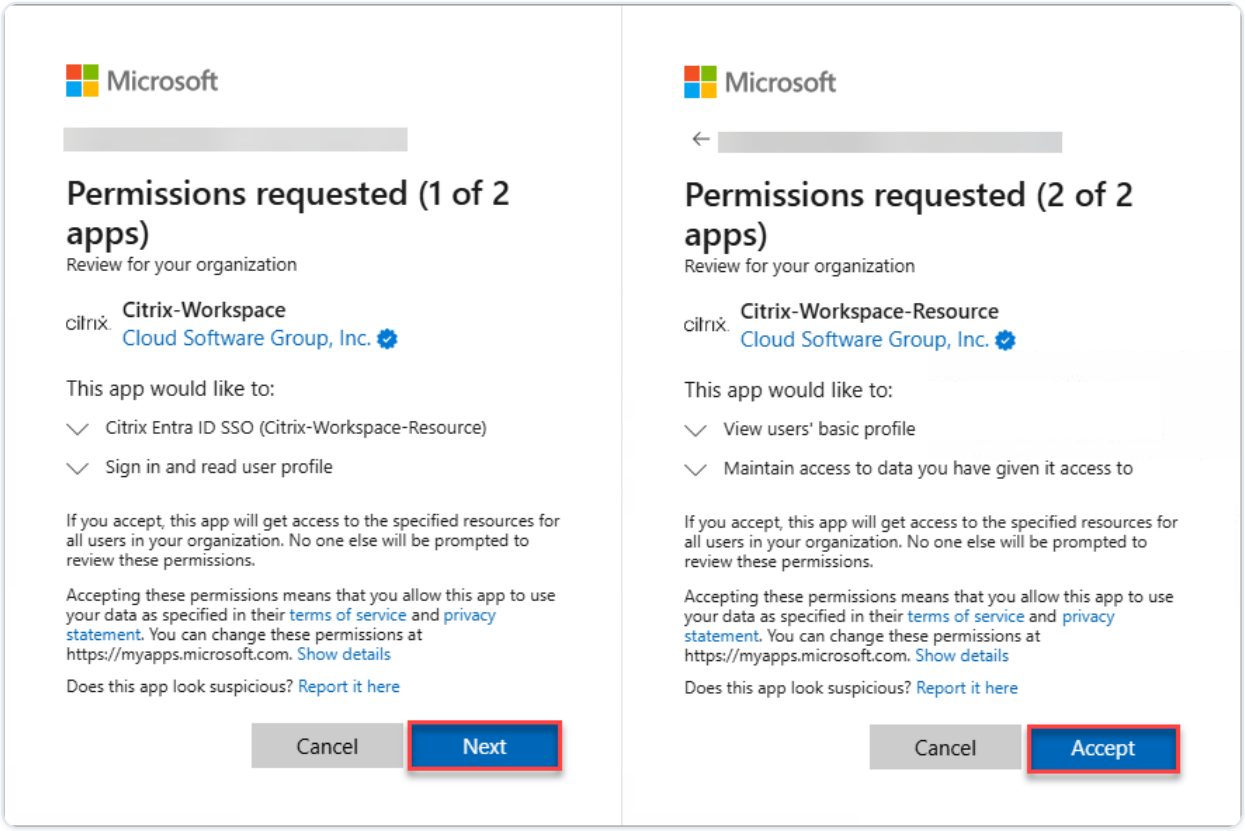
5. Aceite as permissões solicitadas para o aplicativo de Recurso Citrix.



6. Clique em `Register` ao lado de **Registrar aplicativo cliente**.



7. Aceite as permissões solicitadas para o aplicativo Cliente Citrix.



Como alternativa, você pode usar os seguintes URLs de consentimento para registrar os aplicativos. Certifique-se de registrar o aplicativo de Recurso primeiro, seguido pelo aplicativo Cliente.

- Citrix Cloud EUA, UE, APS
  - Aplicativo de recurso: `https://login.microsoftonline.com/common/adminconsent?client_id=3a510bb1-e334-4298-831e-3eac97f8b26c`
  - Aplicativo cliente: `https://login.microsoftonline.com/common/adminconsent?client_id=85651ebe-9a8e-49e4-aaf2-9274d9b6499f`
- Citrix Cloud Japão
  - Aplicativo de recurso: `https://login.microsoftonline.com/common/adminconsent?client_id=0027603f-364b-40f2-98be-8ca4bb79bf8b`
  - Aplicativo cliente: `https://login.microsoftonline.com/common/adminconsent?client_id=0fa97bc0-059c-4c10-8c54-845a1fd5a916`

A seguir estão as permissões dos aplicativos:
Aplicativo de Recurso Citrix
Um principal de serviço é criado com as seguintes permissões:

NOME DA API	VALOR DA REIVINDICAÇÃO	PERMISSÃO	TIPO
Microsoft Graph	User.Read	Entrar e ler perfil de usuário	Delegado

Para Citrix Cloud EUA, UE e APS, o aplicativo é chamado Citrix-Workspace-Resource (application ID 3a510bb1-e334-4298-831e-3eac97f8b26c).

Para Citrix Cloud Japão, o aplicativo é chamado Citrix-Workspace-Resource-JP (application ID 0027603f-364b-40f2-98be-8ca4bb79bf8b).
Aplicativo Cliente Citrix
Um principal de serviço é criado com as seguintes permissões:

NOME DA API	VALOR DA DECLARAÇÃO	PERMISSÃO	TIPO	
Citrix-Workspace-Resource Citrix-Workspace-Resource-JP	user_impersonation	Citrix Entra ID SSO	Delegado	
Microsoft Graph	User.Read	Entrar e ler perfil de usuário	Delegado	

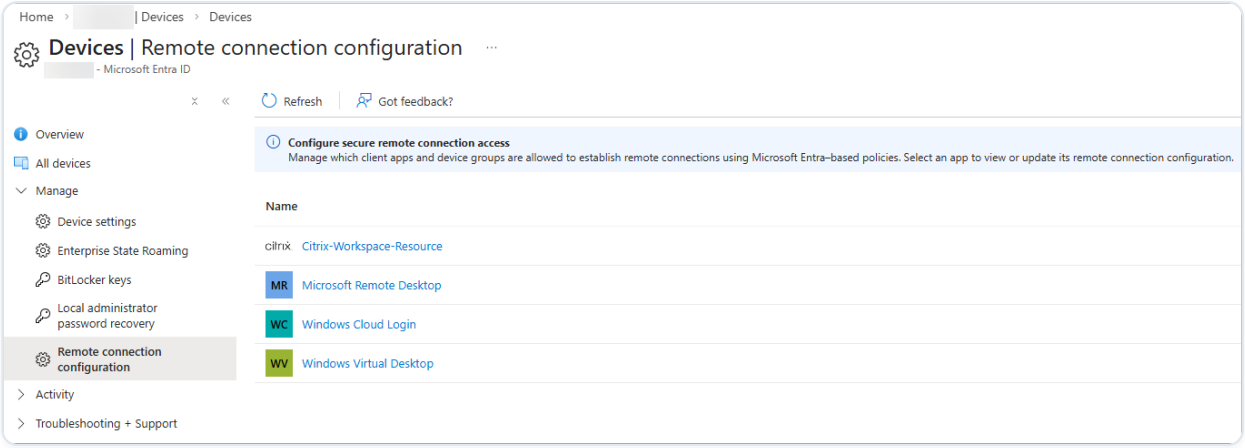
Para Citrix Cloud US, EU e APS, o aplicativo é chamado Citrix-Workspace (ID do aplicativo 85651ebe-9a8e-49e4-aaf2-9274d9b6499f).

Para Citrix Cloud Japan, o aplicativo é chamado Citrix-Workspace-JP (ID do aplicativo 0fa97bc0-059c-4c10-8c54-845a1fd5a916).

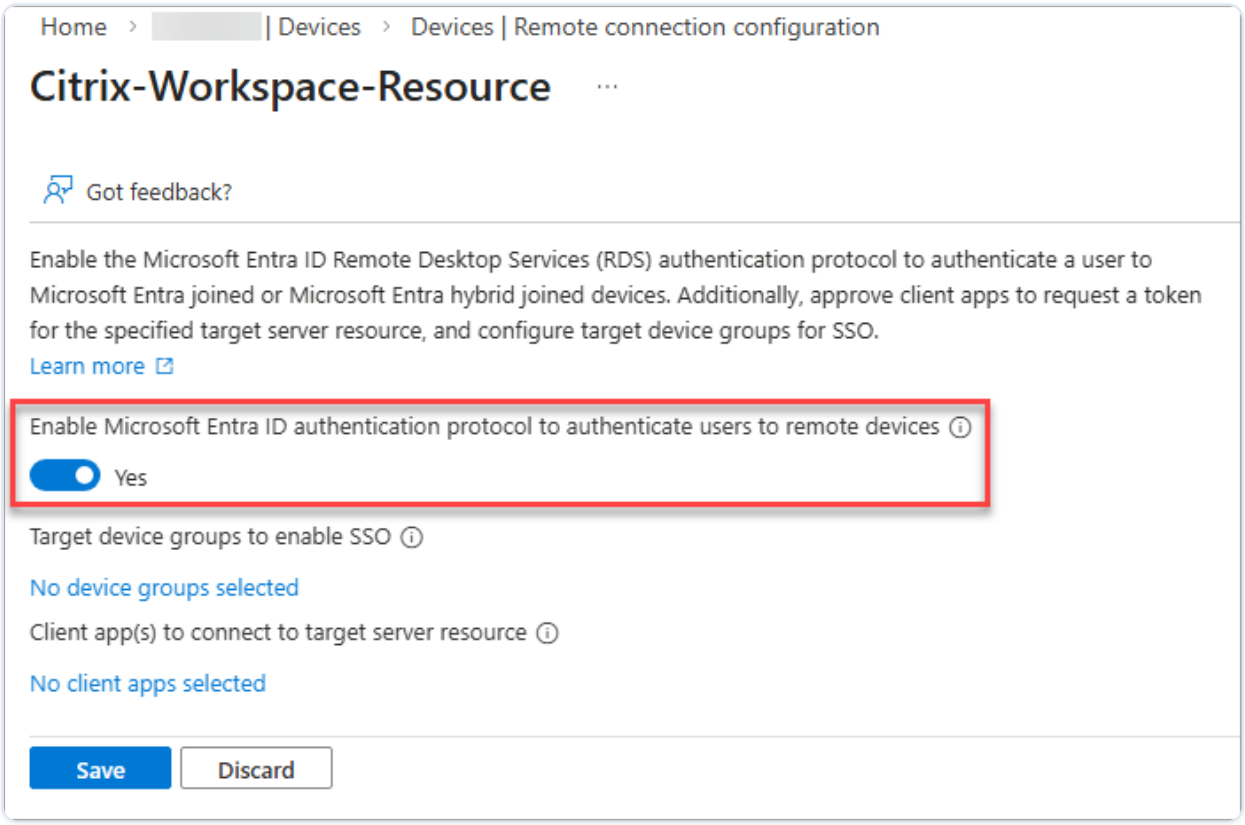
HABILITAR O PROTOCOLO DE AUTENTICAÇÃO DOS SERVIÇOS DE ÁREA DE TRABALHO REMOTA DO MICROSOFT ENTRA ID

Você deve habilitar o protocolo de autenticação dos Serviços de Área de Trabalho Remota do Microsoft Entra ID no aplicativo Citrix Resource. Para fazer isso:

1. No Portal do Azure, navegar para `Microsoft Entra ID` > `Devices` > `Manage` > `Remote connection configuration`.



2. Selecione **Citrix-Workspace-Resource**.
3. Habilite o **protocolo de autenticação dos Serviços de Área de Trabalho Remota do Microsoft Entra ID**.



4. Prossiga para ocultar o prompt de consentimento do usuário.

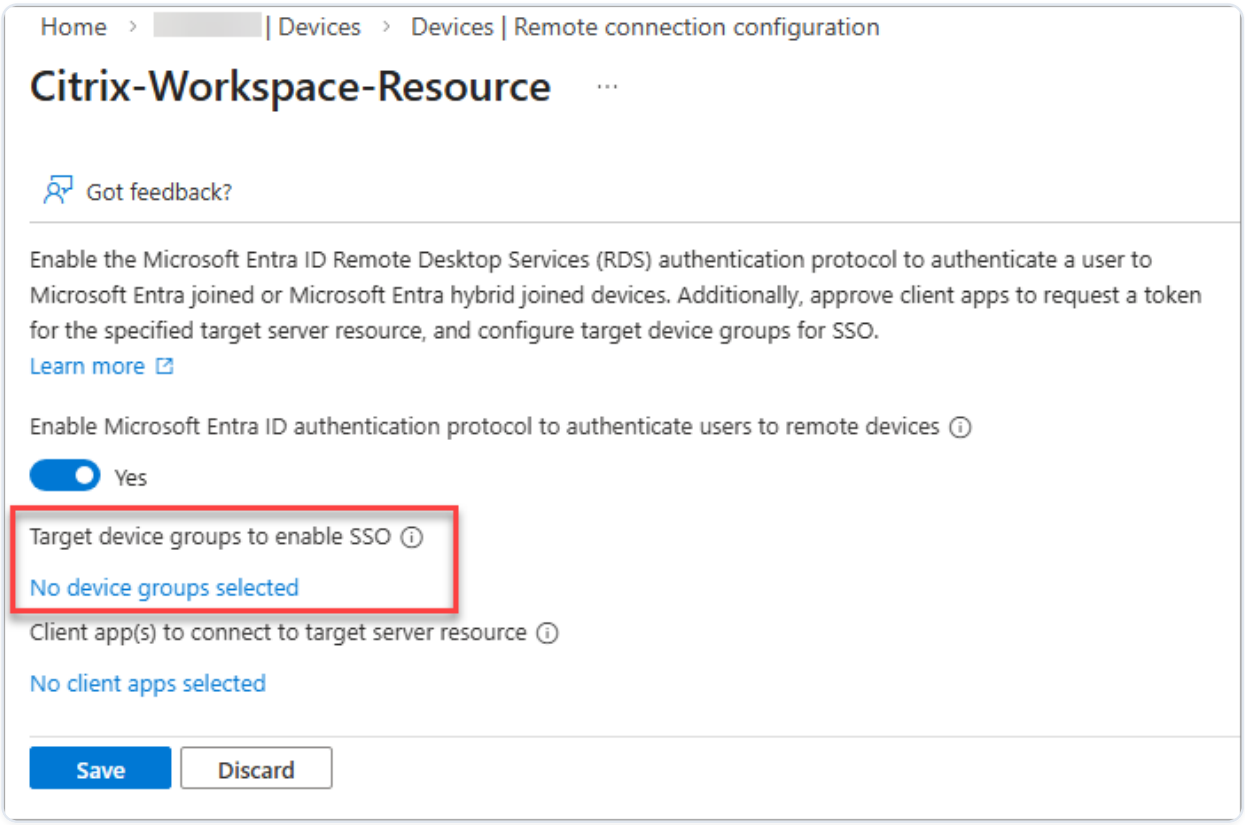
OCULTAR A CAIXA DE DIÁLOGO DO PROMPT DE CONSENTIMENTO DO USUÁRIO

Por padrão, os usuários são solicitados a permitir a conexão de Área de Trabalho Remota ao se conectar a um host de sessão ingressado no Microsoft Entra ou ingressado no Microsoft Entra híbrido com o logon único do Microsoft Entra habilitado, no qual eles devem selecionar **Sim** para permitir o logon único. O Microsoft Entra lembrará até 15 hosts de sessão exclusivos por 30 dias antes de solicitar novamente.

Você pode ocultar esta caixa de diálogo configurando uma lista de dispositivos de destino. Para configurar a lista de dispositivos, você deve criar um ou mais grupos no Microsoft Entra ID que contenham os hosts de sessão ingressados no Microsoft Entra e/ou ingressados no Microsoft Entra híbrido e, em seguida, autorizar os grupos no aplicativo de recurso, até um máximo de 10 grupos.

Depois de habilitar o protocolo de autenticação dos Serviços de Área de Trabalho Remota do Microsoft Entra ID e os grupos terem sido criados:

1. Clique no link para adicionar os grupos de dispositivos de destino e selecione os grupos apropriados.



NOTA

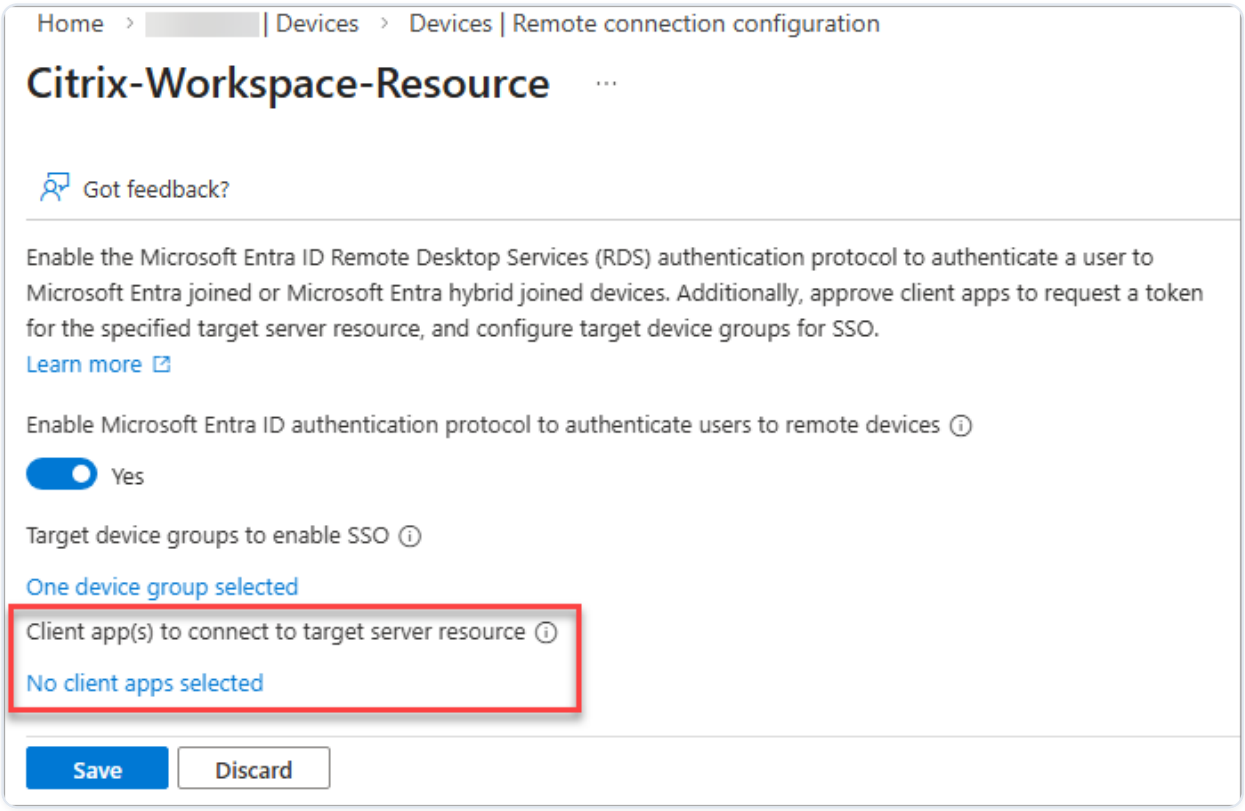
É altamente recomendável criar um grupo dinâmico para simplificar o gerenciamento de membros do grupo. Embora os grupos dinâmicos normalmente sejam atualizados em 5 a 10 minutos, locatários grandes podem levar até 24 horas.

Os grupos dinâmicos exigem a licença Microsoft Entra ID P1 ou a licença Intune for Education. Para obter mais informações, consulte Regras de associação dinâmica para grupos.

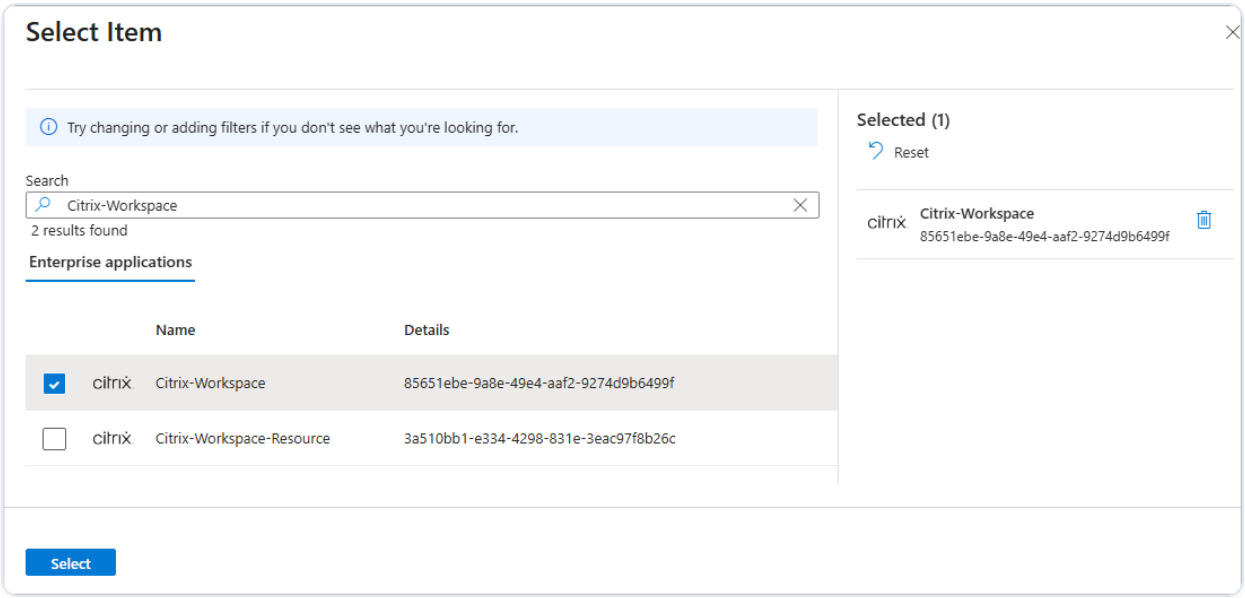
APROVAR O APLICATIVO CLIENTE

Você deve adicionar explicitamente o aplicativo Citrix Client como um cliente aprovado no aplicativo Citrix Resource:

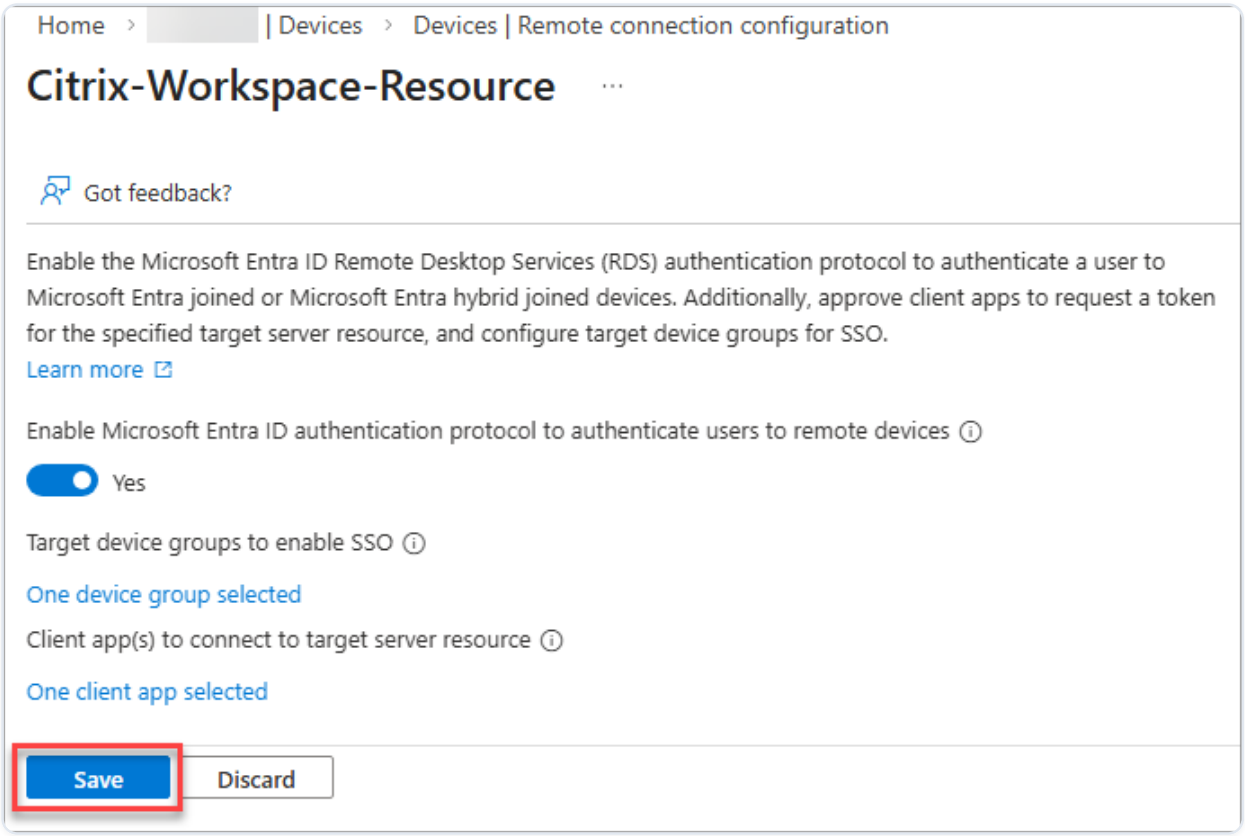
1. Clique no link para adicionar seus aplicativos cliente confiáveis.



2. Selecione o aplicativo Citrix Client.



3. Selecione **Salvar** para aplicar as alterações de configuração ao aplicativo Citrix Resource.



CRIAR UM OBJETO DE SERVIDOR KERBEROS

Se seus hosts de sessão são ingressados no Microsoft Entra híbrido, você deve configurar um objeto de servidor Kerberos no domínio do Active Directory onde as contas de usuário e computador residem. Consulte Criar um objeto de servidor Kerberos para obter detalhes.

REVISAR POLÍTICAS DE ACESSO CONDICIONAL DO MICROSOFT ENTRA

Se você usa ou planeja usar políticas de Acesso Condicional do Microsoft Entra, elas precisam ser aplicadas ao aplicativo de Recurso Citrix.

Para obter orientações detalhadas sobre como configurar o Acesso Condicional ao usar o logon único do Microsoft Entra para DaaS, consulte a documentação da Microsoft. Lembre-se de que as configurações de Acesso Condicional necessárias devem ser aplicadas ao **aplicativo de Recurso Citrix**, e não ao aplicativo Cliente Citrix ou aos aplicativos Microsoft.

Configuração Citrix

HOSTS DE SESSÃO CITRIX

Certifique-se de que os requisitos de sistema para os hosts de sessão sejam atendidos:

1. Certifique-se de que os hosts de sessão sejam ingressados no Microsoft Entra ou ingressados no Microsoft Entra híbrido.

2. Instale a versão e o build do sistema operacional necessários, conforme especificado nos requisitos do sistema.
3. Instale a versão do VDA necessária, conforme especificado nos requisitos do sistema.

Hosts de sessão ingressados no Microsoft Entra híbrido
Se você estiver implantando hosts de sessão ingressados no Microsoft Entra híbrido com Citrix Machines Creation Services, Citrix Provisioning ou Windows 365, você pode prosseguir para a próxima seção. Se você estiver provisionando hosts ingressados no Microsoft Entra híbrido usando qualquer outra ferramenta ou método, você deve adicionar o seguinte valor de registro aos seus hosts de sessão:

- Chave: `HKLM\SYSTEM\CurrentControlSet\Control\Citrix`
- Tipo de valor: **DWORD**
- Nome do valor: `AzureADJoinType`
- Dados: `1`

Comportamento de bloqueio de sessão
Quando um desktop virtual é bloqueado, o comportamento padrão é exibir a tela de bloqueio do Windows. Neste ponto, os métodos de autenticação suportados para desbloquear o desktop são **nome de usuário e senha** ou **cartão inteligente**.

> **NOTA**

> O logon web da Citrix (visualização) permite que você desbloqueie seu desktop usando a autenticação Entra baseada na web. Consulte Logon web para obter detalhes.

> Se você tiver uma implantação sem senha onde os usuários não sabem suas senhas, é recomendável configurar o comportamento de bloqueio de sessão para desconectar a sessão em vez de mostrar a tela de bloqueio.

- **Hosts de sessão multi-sessão**

  Você pode configurar esse comportamento habilitando a configuração **Desconectar sessão remota no bloqueio para autenticação da plataforma de identidade da Microsoft** através do Intune ou da Política de Grupo. Para obter etapas detalhadas, consulte Configurar o comportamento de bloqueio de sessão para o Azure Virtual Desktop.

- **Hosts de sessão de sessão única**

Se você estiver usando o **VDA versão 2603 ou mais recente**, você pode configurar esse comportamento habilitando a configuração **Desconectar sessão remota no bloqueio para autenticação da plataforma de identidade da Microsoft** através do Intune ou da Política de Grupo. Para obter etapas detalhadas, consulte Configurar o comportamento de bloqueio de sessão para o Azure Virtual Desktop.

Se você estiver usando o VDA versão 2511 ou mais antigo, a configuração **Desconectar sessão remota no bloqueio para autenticação da plataforma de identidade da Microsoft** não é suportada. No entanto, você pode obter o mesmo comportamento criando uma tarefa agendada do Windows.

O script de exemplo a seguir cria uma tarefa agendada em hosts de sessão única que executa `cmd.exe /c tsdiscon` quando o desktop é bloqueado:

```
# Create the TaskService COM object

$service = New-Object -ComObject "Schedule.Service"

$service.Connect()



# Get the root folder and create a new task definition

$rootFolder = $service.GetFolder("\")

$taskDef = $service.NewTask(0)



# Registration info

$taskDef.RegistrationInfo.Description = "Disconnect session when
workstation is locked"



# Principal (Users group, least privilege)

$principal = $taskDef.Principal

$principal.GroupId = "S-1-5-32-545"
```

```
$principal.RunLevel = 0  # 0 = LeastPrivilege



# Settings
$settings = $taskDef.Settings
$settings.Enabled = $true
$settings.AllowDemandStart = $true
$settings.DisallowStartIfOnBatteries = $false
$settings.StopIfGoingOnBatteries = $false
$settings.AllowHardTerminate = $false
$settings.StartWhenAvailable = $false
$settings.RunOnlyIfNetworkAvailable = $false
$settings.IdleSettings.StopOnIdleEnd = $true
$settings.IdleSettings.RestartOnIdle = $false
$settings.Hidden = $false
$settings.RunOnlyIfIdle = $false
$settings.DisallowStartOnRemoteAppSession = $false
$settings.UseUnifiedSchedulingEngine = $true
$settings.WakeToRun = $false
$settings.ExecutionTimeLimit = "PT0S"   # Unlimited
$settings.Priority = 7
$settings.MultipleInstances = 1         # IgnoreNew
```

```
# Trigger: SessionLock

$trigger = $taskDef.Triggers.Create(11)  # 11 =
TASK_TRIGGER_SESSION_STATE_CHANGE

$trigger.StateChange = 7                 # 7 = SessionLock

$trigger.Enabled = $true



# Action: tsdiscon

$action = $taskDef.Actions.Create(0)     # 0 = Exec

$action.Path = "cmd.exe"

$action.Arguments = "/c tsdiscon"



# Register the task

$rootFolder.RegisterTaskDefinition(

    "Disconnect on Lock",  # Task name

    $taskDef,

    6,                     # TASK_CREATE_OR_UPDATE

    $null, $null,          # No specific user/password

    3                      # TASK_LOGON_GROUP

) | Out-Null
```

Se você precisar remover a tarefa agendada posteriormente, você pode executar o seguinte comando:

```
Unregister-ScheduledTask -TaskName "Disconnect on Lock" -Confirm:$false
```

PLANO DE ACESSO E CONTROLE CITRIX

Autenticação do Workspace

Você deve configurar o Citrix® StoreFront Cloud para usar o Microsoft Entra ID ou SAML como IdP. Consulte a documentação do Citrix® StoreFront Cloud para obter detalhes.

> **NOTA**
>
> Se você planeja usar SAML como seu IdP, deve garantir que seu provedor SAML esteja configurado corretamente para oferecer suporte à autenticação baseada em Entra. Consulte SAML usando Microsoft Entra ID e identidades do Microsoft Entra para autenticação.

Gerenciando o acesso ao Workspace

Se seus usuários acessarem sua loja por meio de um navegador da web, nenhuma configuração adicional será necessária. Se você quiser impor o acesso nativo, poderá configurar o Citrix® StoreFront Cloud para `Require end users to access their store from the Citrix client app` em configuração de acesso da loja.

Habilitando o logon único do Microsoft Entra no Workspace

Após a configuração da autenticação, você deve habilitar o uso do logon único do Microsoft Entra:

1. Crie um principal de serviço no Citrix Cloud:
    a. Vá para **Gerenciamento de identidade e acesso > Acesso à API > Principais de serviço**.
    b. Clique em **Criar principal de serviço**.
    c. Insira um **nome** para o principal de serviço e clique em **Avançar**.
    d. Defina o acesso para o principal de serviço:
        i. Selecione **Acesso total**, ou
        ii. Selecione **Acesso personalizado > Geral > Citrix® StoreFront Cloud** e clique em **Avançar**.
    e. Defina o **tempo de expiração** do segredo e clique em **Avançar**.
    f. Clique em **Concluir**.
    g. Salve o segredo e o ID.
2. Baixe e extraia o módulo Citrix® StoreFront Cloud PowerShell para sua estação de trabalho, ou qualquer máquina que você possa usar para fins administrativos.

3. Abra o PowerShell na máquina em que você baixou o módulo Citrix® StoreFront Cloud PowerShell.
4. Execute os seguintes comandos:

```
Import-Module -Name
“<extractedPath>\Citrix.Workspace.StoreConfigs.psm1”

Set-StoreConfigurations -StoreUrl "https://
<yourPrimaryStore>.cloud.com" -ClientId "<clientId>" -ClientSecret
"<clientSecret>" -AzureAdSsoEnabled $True
```

> **NOTA:**
>
> Esta é uma configuração global que será aplicada a todas as lojas no seu locatário do Citrix Cloud. Atualmente, não é possível habilitar ou desabilitar esta configuração em lojas específicas com base na URL da loja fornecida no comando.

5. Execute o seguinte comando para verificar se a configuração foi feita corretamente:

```
Get-StoreConfigurations -StoreUrl "https://
<yourPrimaryStore>.cloud.com" -ClientId "<clientId>" -ClientSecret
"<clientSecret>"
```

Configuração do grupo de entrega

1. Se seus hosts de sessão forem ingressados no Microsoft Entra híbrido, atribua os aplicativos virtuais e/ou desktops aos usuários ou grupos apropriados do Microsoft Entra. Quaisquer atribuições existentes a usuários ou grupos do Active Directory podem ser removidas, mas não é obrigatório.
2. Se você estiver provisionando seus hosts de sessão ingressados no Microsoft Entra com algo diferente de Citrix Machine Creation Services, Citrix Provisioning ou Windows 365, você precisará configurar o tipo de logon para os Grupos de Entrega. Se você estiver usando hosts de sessão ingressados no Microsoft Entra híbrido, o tipo de logon para o grupo de entrega deve ser configurado independentemente do método de provisionamento.

a. Se você ainda não tem o SDK do Citrix Remote PowerShell instalado, baixe-o e instale-o em sua estação de trabalho, ou em qualquer máquina que você possa usar para fins administrativos.

b. Abra um prompt do PowerShell na máquina em que você instalou o SDK do Citrix Remote PowerShell.

c. Execute os seguintes comandos:

Ingressado no Microsoft Entra

```
asnp citrix*

Get-XDAuthentication

Get-BrokerDesktopGroup -Name <dgName> | Set-BrokerDesktopGroup
-MachineLogOnType "AzureAd"
```

Microsoft Entra unido hibridamente

```
asnp citrix*

Get-XDAuthentication

Get-BrokerDesktopGroup -Name <dgName> | Set-BrokerDesktopGroup
-MachineLogOnType "HybridAzureAd"
```

Configurando o logon único do Microsoft Entra no VDA
Por padrão, o logon único do Microsoft Entra está habilitado no VDA. Para habilitar ou desabilitar essa capacidade para um subconjunto de hosts de sessão, use a configuração de política de logon único do Microsoft Entra.

DISPOSITIVO CLIENTE

Certifique-se de que os requisitos de sistema para os dispositivos cliente sejam atendidos:

1. Instale a versão necessária do aplicativo Citrix Workspace conforme especificado nos requisitos de sistema.
2. Se seus usuários estiverem aproveitando o acesso híbrido, certifique-se de que a Extensão Web do Citrix esteja instalada. Se seus usuários estiverem usando acesso nativo ou via navegador, a Extensão Web do Citrix não será necessária.

Solução de problemas

Problemas conhecidos

- Após habilitar o logon único do Microsoft Entra, os usuários podem encontrar o erro da Microsoft **AADSTS293005** ao iniciar seu desktop virtual, indicando `RDP protocol is not enabled for the requested resource application. Please configure the RemoteDesktopSecurityConfiguration property on resource service principal to enable RDP protocol.` Para resolver esse problema, reinicie o aplicativo Citrix Workspace.
- Os usuários podem encontrar um atraso de 30 segundos ao iniciar sessões se o aplicativo Citrix Workspace não suportar o logon único do Microsoft Entra ou se usarem acesso híbrido sem a Extensão Web do Citrix.
- Os usuários podem encontrar um atraso de 30 segundos ao iniciar sessões se o logon único do Microsoft Entra estiver habilitado no Citrix® StoreFront Cloud e a configuração necessária do Azure não tiver sido concluída.
- Se a configuração **Autenticação de reconexão automática do cliente** estiver habilitada, o logon único falhará. Como solução alternativa, desabilite essa configuração nos hosts de sessão relevantes.
- Se **Manter-me conectado (KMSI)** estiver desabilitado no Entra ID, o logon único falhará em dispositivos cliente Linux e macOS.

Quando o logon único falha

Se o logon único falhar ao acessar desktops ou aplicativos virtuais, proceda da seguinte forma:

1. Confirme se o logon único do Microsoft Entra está habilitado no Citrix® StoreFront Cloud.
2. Confirme se o método de acesso utilizado pelo usuário é compatível.
3. Se o usuário estiver utilizando acesso híbrido, confirme se a Extensão Web do Citrix está instalada.
4. Confirme se o dispositivo cliente está executando a versão necessária do aplicativo Citrix Workspace.
5. Confirme se seus hosts de sessão estão executando a compilação do Windows necessária.
6. Confirme se seus hosts de sessão estão executando a versão VDA necessária.
7. Certifique-se de que a configuração do Windows `Always prompt for password upon connection` não esteja habilitada nos hosts de sessão.

Essa configuração é desabilitada por padrão e pode ser configurada por meio da Política de Grupo ou do Intune em `Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security`.

Você pode proteger o registro para verificar se a configuração está habilitada procurando pelo valor `fPromptForPassword` em `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services`. Se o valor estiver definido como `1`, a configuração estará habilitada e o logon único não estará disponível. Se o valor estiver ausente ou definido como `0`, a configuração estará desabilitada.

8. Certifique-se de que a configuração do Windows `Allow Custom SSPs and APs to be loaded into LSASS` esteja habilitada nos hosts de sessão. Essa configuração é habilitada por padrão e pode ser configurada por meio da Política de Grupo ou do Intune em `Computer Configuration\System\Local Security Authority`.
9. Confirme se a configuração `AzureADJoinType` está configurada corretamente nos hosts de sessão:
   - Chave: `HKLM\SYSTEM\CurrentControlSet\Control\Citrix`
   - Tipo de valor: **DWORD**
   - Nome do valor: `AzureADJoinType`
   - Dados do valor: `1` (Microsoft Entra híbrido unido); `2` (Microsoft Entra unido)
10. Certifique-se de que os desktops virtuais ou aplicativos sejam atribuídos a identidades do Microsoft Entra em vez de identidades do Active Directory no Citrix Studio.
11. Confirme se o tipo de logon dos Delivery Groups está configurado corretamente executando o seguinte comando PowerShell:

    ```
    Get-BrokerDesktopGroup -Name <deliveryGroupName>
    ```

    Para hosts de sessão unidos ao Microsoft Entra, `MachineLogOnType` deve ser definido como `AzureAd`. Para hosts de sessão unidos ao Microsoft Entra híbrido, `MachineLogOnType` deve ser definido como `HybridAzureAd`.
12. Se você estiver usando um IdP SAML, confirme se a configuração necessária foi implementada.
13. Confirme se os aplicativos Citrix Resource e Client estão registrados no locatário do Microsoft Entra.

14. Confirme se o protocolo de autenticação RDS do Microsoft Entra ID está habilitado no aplicativo Citrix Resource.
15. Confirme se o aplicativo Citrix Client foi adicionado como um aplicativo cliente aprovado no aplicativo Citrix Resource.
16. Se seus hosts de sessão forem unidos ao Microsoft Entra híbrido, confirme se um objeto de servidor Kerberos foi criado no domínio do Active Directory onde as contas de usuário e computador residem.
17. Revise suas políticas de Acesso Condicional do Microsoft Entra. Certifique-se de que nenhuma política esteja sendo aplicada ao aplicativo Citrix Client e que quaisquer políticas aplicadas ao aplicativo Citrix Resource ou aos hosts de sessão estejam configuradas corretamente para que não afetem a experiência de logon único.

Configuração do Azure para logon único do Microsoft Entra

Para aproveitar o logon único do Microsoft Entra, você deve primeiro permitir a autenticação do Microsoft Entra para Windows em seu locatário do Microsoft Entra ID, o que permite a emissão dos tokens de autenticação necessários que permitem aos usuários fazer login nos hosts de sessão ingressados no Microsoft Entra e ingressados no Microsoft Entra híbrido. Para conseguir isso, você deve fazer o seguinte:

1. Registre os aplicativos Citrix (aplicativo de Recurso e aplicativo Cliente) em seu locatário do Microsoft Entra ID.
2. Habilite a Configuração de Segurança da Área de Trabalho Remota para o aplicativo de recurso Citrix.
3. Adicione o aplicativo cliente Citrix como um cliente aprovado para o aplicativo de recurso Citrix.
4. \[Opcional\] Ocultar a caixa de diálogo de solicitação de consentimento do usuário.
5. Crie um objeto de servidor Kerberos.
6. Revise as políticas de Acesso Condicional do Microsoft Entra.

A pessoa que realiza a configuração do Azure deve ter atribuída uma das seguintes funções internas do Microsoft Entra ou equivalente, no mínimo:

- Administrador de Aplicativos
- Administrador de Aplicativos na Nuvem

Se você deseja concluir a configuração do Azure via PowerShell, precisará usar o SDK do Microsoft Graph PowerShell. Você também pode aproveitar a API do Microsoft Graph com uma ferramenta como o Graph Explorer.

São fornecidas instruções sobre como concluir a configuração com PowerShell e Graph Explorer.

Configuração do PowerShell

Se você optar por usar o SDK do Microsoft Graph PowerShell, observe:

- Você precisará usar o Azure Cloud Shell com o tipo de terminal PowerShell, ou executar o PowerShell 7.x em seu sistema local, e garantir que seu contexto do Azure esteja definido para a assinatura que você deseja usar.
- Você precisará instalar o módulo Microsoft Graph PowerShell SDK v1.0 (Microsoft.Graph) e o módulo de aplicativo beta (Microsoft.Graph.Beta.Applications).

HABILITAR CONFIGURAÇÃO DE SEGURANÇA DE ÁREA DE TRABALHO REMOTA

Depois de registrar os aplicativos Citrix, você deve habilitar a Configuração de Segurança de Área de Trabalho Remota no aplicativo Citrix Resource.

1. Importe os módulos de Autenticação e Aplicativo do Microsoft Graph e conecte-se ao Microsoft Graph com os escopos `Application.Read.All` e `Application-RemoteDesktopConfig.ReadWrite.All`:

   ```
   Import-Module Microsoft.Graph.Authentication

   Import-Module Microsoft.Graph.Applications

   Import-Module Microsoft.Graph.Beta.Applications

   Connect-MgGraph -Scopes "Application.Read.All","Application-
   RemoteDesktopConfig.ReadWrite.All"
   ```

2. Obtenha o ID do objeto para os principais de serviço associados aos registros de aplicativo:

   Citrix Cloud EUA, UE, APS

   ```
   $CtxResourceSpId = (Get-MgServicePrincipal -Filter "AppId eq '3a510bb1-
   e334-4298-831e-3eac97f8b26c'").Id
   ```

```
$CtxClientSpId = (Get-MgServicePrincipal -Filter "AppId eq
'85651ebe-9a8e-49e4-aaf2-9274d9b6499f'").Id
```

Citrix Cloud Japão

```
$CtxResourceSpId = (Get-MgServicePrincipal -Filter "AppId eq
'0027603f-364b-40f2-98be-8ca4bb79bf8b'").Id

$CtxClientSpId = (Get-MgServicePrincipal -Filter "AppId eq
'0fa97bc0-059c-4c10-8c54-845a1fd5a916'").Id
```

3. Defina a propriedade `isRemoteDesktopProtocolEnabled` como `true`:

```
If ((Get-MgServicePrincipalRemoteDesktopSecurityConfiguration
-ServicePrincipalId $CtxResourceSpId) -ne $true) {

    Update-MgServicePrincipalRemoteDesktopSecurityConfiguration
-ServicePrincipalId $CtxResourceSpId -IsRemoteDesktopProtocolEnabled

}
```

4. Confirme se a propriedade `isRemoteDesktopProtocolEnabled` está definida como `true`:

```
Get-MgServicePrincipalRemoteDesktopSecurityConfiguration
-ServicePrincipalId $CtxResourceSpId
```

APROVAR O APLICATIVO CLIENTE

Você deve adicionar explicitamente o aplicativo Citrix Client como um cliente aprovado no aplicativo Citrix Resource.

1. Crie um objeto `approvedClientApp`:

```
$acp = New-Object -TypeName
Microsoft.Graph.Beta.PowerShell.Models.MicrosoftGraphApprovedClientApp

$acp.Id = $CtxClientSpId
```

2. Adicione o aplicativo cliente ao objeto `approvedClientApp`:

```
New-
MgBetaServicePrincipalRemoteDesktopSecurityConfigurationApprovedClientA
pp -ServicePrincipalId $CtxResourceSpId -BodyParameter $acp
```

A saída deve ser semelhante a esta:

```
Id                                   DisplayName

--                                   -----------

87654321-wxyz-1a2b-3c4d-1029384756af  Citrix-Workspace
```

OCULTAR A CAIXA DE DIÁLOGO DE SOLICITAÇÃO DE CONSENTIMENTO DO USUÁRIO

Por padrão, os usuários são solicitados a permitir a conexão de Área de Trabalho Remota ao se conectar a um host de sessão ingressado no Microsoft Entra ou ingressado no Microsoft Entra híbrido com logon único do Microsoft Entra habilitado, no qual eles devem selecionar Sim para permitir o logon único. O Microsoft Entra lembrará até 15 hosts de sessão exclusivos por 30 dias antes de solicitar novamente.

Você pode ocultar esta caixa de diálogo configurando uma lista de dispositivos de destino. Para configurar a lista de dispositivos, você deve criar um ou mais grupos no Microsoft Entra ID que contenham os hosts de sessão ingressados no Microsoft Entra e/ou ingressados no Microsoft Entra híbrido e, em seguida, autorizar os grupos no aplicativo de recurso, até um máximo de 10 grupos.

NOTA

É altamente recomendável criar um grupo dinâmico para simplificar o gerenciamento de associação para o grupo. Embora os grupos dinâmicos normalmente sejam atualizados em 5 a 10 minutos, locatários grandes podem levar até 24 horas.

Grupos dinâmicos exigem a licença Microsoft Entra ID P1 ou a licença Intune for Education. Para obter mais informações, consulte Regras de associação dinâmica para grupos.

Depois que os grupos forem criados, siga estas etapas:

1. Obtenha o ID do objeto (OID) do grupo que contém os hosts de sessão para os quais você deseja ocultar o prompt de conexão da Área de Trabalho Remota.
2. Crie um objeto `targetDeviceGroup`:

```
$tdg = New-Object -TypeName
Microsoft.Graph.PowerShell.Models.MicrosoftGraphTargetDeviceGroup

$tdg.Id = "<groupOID>"
```

3. Adicione o aplicativo cliente ao objeto `approvedClientApp`:

```
New-
MgServicePrincipalRemoteDesktopSecurityConfigurationTargetDeviceGroup
-ServicePrincipalId $CtxResourceSpId -BodyParameter $tdg
```

   A saída deve ser semelhante a esta:

```
Id                                   DisplayName

--                                   -----------

87654321-wxyz-1a2b-3c4d-1029384756af  Entra-SSO-Desktops
```

4. Se você precisar remover um grupo de dispositivos do objeto targetDeviceGroup posteriormente, execute o seguinte comando:

```
Remove-
MgServicePrincipalRemoteDesktopSecurityConfigurationTargetDeviceGroup
-ServicePrincipalId $CtxResourceSpId -TargetDeviceGroupId "<groupOID>"
```

NOTA

Você pode repetir estas etapas para adicionar mais grupos, se necessário, até um máximo de 10 grupos.

Configuração da API do Microsoft Graph

HABILITAR CONFIGURAÇÃO DE SEGURANÇA DA ÁREA DE TRABALHO REMOTA

Depois de (/pt-br/citrix-daas/install-configure/session-authentication/entra-sso.html#register-citrix-applications) , você deve habilitar a Configuração de Segurança da Área de Trabalho Remota no aplicativo de Recurso Citrix.

1. Obtenha o ID do objeto (OID) para os principais de serviço associados aos registros de aplicativo no portal do Azure:
   a. navegar até Microsoft Entra ID > Aplicativos Empresariais.
   b. Remova o filtro `Application type`, se definido, para que todos os aplicativos sejam listados.
   c. Pesquise por `Citrix-Workspace-Resource` / `Citrix-Workspace-Resource-JP` e anote o ID do objeto associado para o aplicativo de Recurso.
   d. Pesquise por `Citrix-Workspace` / `Citrix-Workspace-JP` e anote o ID do objeto associado para o aplicativo cliente.
2. No Graph Explorer, faça login com uma conta do locatário do Azure de destino que tenha as permissões necessárias.
3. Defina a seguinte consulta:
   - Método de solicitação HTTP: PATCH
   - Versão da API do Microsoft Graph: v1.0
   - Consulta:

     ```
     https://graph.microsoft.com/v1.0/servicePrincipals/<resourceAppOID>/
     remoteDesktopSecurityConfiguration
     ```

   - Corpo da solicitação:

     ```
     {

         "@odata.type":
     "#microsoft.graph.remoteDesktopSecurityConfiguration",

         "isRemoteDesktopProtocolEnabled": true
     ```

```
}
```

4. Selecione a guia **Modificar Permissões** e certifique-se de ter consentido com a permissão `Application.ReadWrite.All`.
5. Execute a consulta.

Consulte o tipo de recurso remoteDesktopSecurityConfiguration para referência.

APROVAR O APLICATIVO CLIENTE

Você deve adicionar explicitamente o aplicativo Citrix Client como um cliente aprovado no aplicativo Citrix Resource.

Defina a seguinte consulta e execute-a:

- Método de solicitação HTTP: POST
- Versão da API do Microsoft Graph: v1.0
- Consulta:

```
https://graph.microsoft.com/v1.0/servicePrincipals/<resourceAppOID>/
remoteDesktopSecurityConfiguration/approvedClientApps
```

- Corpo da solicitação:

```
{

    "@odata.type": "#microsoft.graph.approvedClientApp",

    "id": "<clientAppOID>"

}
```

OCULTAR A CAIXA DE DIÁLOGO DE SOLICITAÇÃO DE CONSENTIMENTO DO USUÁRIO

Por padrão, os usuários são solicitados a permitir a conexão de Área de Trabalho Remota ao se conectar a um host de sessão ingressado no Microsoft Entra ou ingressado no Microsoft Entra híbrido com o logon único do Microsoft Entra habilitado, no qual eles devem selecionar Sim para permitir o logon único. O Microsoft Entra lembrará até 15 hosts de sessão exclusivos por 30 dias antes de solicitar novamente.

Você pode ocultar esta caixa de diálogo configurando uma lista de dispositivos de destino. Para configurar a lista de dispositivos, você deve criar um ou mais grupos no Microsoft Entra ID que contenham os hosts de sessão ingressados no Microsoft Entra e/ou ingressados no Microsoft Entra híbrido e, em seguida, autorizar os grupos no aplicativo de recurso, até um máximo de 10 grupos.

> **NOTA**
>
> É altamente recomendável criar um grupo dinâmico para simplificar o gerenciamento de membros do grupo. Embora os grupos dinâmicos normalmente sejam atualizados em 5 a 10 minutos, locatários grandes podem levar até 24 horas.
>
> Grupos dinâmicos exigem a licença Microsoft Entra ID P1 ou a licença Intune for Education. Para obter mais informações, consulte Regras de associação dinâmica para grupos.
>
> Depois que os grupos forem criados, siga estas etapas:

1. Obtenha o ID do objeto (OID) do grupo que contém os hosts de sessão para os quais você deseja ocultar o prompt de conexão da Área de Trabalho Remota.
2. Defina a seguinte consulta e execute-a:
   - Método de solicitação HTTP: POST
   - Versão da API do Microsoft Graph: v1.0
   - Consulta:

     ```
     https://graph.microsoft.com/v1.0/servicePrincipals/<resourceAppOID>/
     remoteDesktopSecurityConfiguration/targetDeviceGroups
     ```

   - Corpo da solicitação:

     ```
     {

         "@odata.type": "#microsoft.graph.targetDeviceGroup",

         "id": "<groupOID>"
     ```

```
}
```

NOTA

Você pode repetir estas etapas para adicionar mais grupos, se necessário, até um máximo de 10 grupos.

Se você precisar remover um grupo de dispositivos mais tarde do objeto targetDeviceGroup, defina o seguinte e execute a consulta:

- Método de solicitação HTTP: DELETE
- Versão da API do Microsoft Graph: v1.0
- Consulta:

```
https://graph.microsoft.com/beta/servicePrincipals/<resourceAppOID>/
remoteDesktopSecurityConfiguration/targetDeviceGroups
```

Consulte tipo de recurso targetDeviceGroup para referência.

CRIAR UM OBJETO DE SERVIDOR KERBEROS

Se seus hosts de sessão forem ingressados no Microsoft Entra híbrido, você deve configurar um objeto de servidor Kerberos no domínio do Active Directory onde as contas de usuário e computador residem. Consulte Criar um objeto de servidor Kerberos para obter detalhes.

REVISAR POLÍTICAS DE ACESSO CONDICIONAL DO MICROSOFT ENTRA

Se você usa ou planeja usar políticas de Acesso Condicional do Microsoft Entra, revise a configuração aplicada ao **aplicativo de Recurso Citrix** e ao **aplicativo Cliente Citrix** para garantir que os usuários tenham a experiência de logon desejada.

Para obter orientações detalhadas sobre a configuração do Acesso Condicional ao usar o logon único do Microsoft Entra para DaaS, consulte a documentação da Microsoft. Lembre-se de que as configurações de Acesso Condicional necessárias devem ser aplicadas ao **aplicativo de Recurso Citrix** ou ao **aplicativo Cliente Citrix**, e não aos aplicativos da Microsoft.

Serviço de Autenticação Federada

O Citrix Federated Authentication Service (FAS) permite o logon único (SSO) em desktops e aplicativos virtuais Citrix em ambientes onde os usuários autenticar por meio de provedores de identidade modernos, como SAML ou OpenID Connect (OIDC), que não fornecem uma senha do Windows, garantindo acesso contínuo a hosts de sessão unidos a um domínio do Active Directory.

Consulte a documentação do Serviço de Autenticação Federada para obter mais detalhes.

Cartões inteligentes

O Citrix Virtual Apps and Desktops e o Citrix DaaS oferecem suporte a cartões inteligentes tanto para fazer login em desktops e aplicativos virtuais quanto para uso em sessões ativas. Os cartões inteligentes fornecem autenticação de dois fatores baseada em certificado que fortalece a segurança, exigindo tanto o cartão físico quanto um PIN. Isso permite que as organizações atendam aos requisitos de conformidade, protejam dados confidenciais e simplifiquem o acesso para usuários que já dependem de cartões inteligentes para logon no Windows ou aplicativos seguros. Uma vez autenticados, os usuários também podem usar seus cartões inteligentes dentro da sessão para assinar documentos digitalmente, criptografar e-mails ou acessar outros aplicativos habilitados para cartão inteligente, garantindo uma experiência consistente e segura em ambientes locais e virtuais.

Consulte a documentação de cartões inteligentes para obter mais detalhes.

Login via web

Você pode usar o provedor de credenciais de login via web do Citrix para habilitar o uso da autenticação Windows baseada em Entra ID. Isso permite que os usuários façam login ou desbloqueiem seus desktops virtuais usando qualquer método de autenticação habilitado no Entra ID.

> **IMPORTANTE**
>
> O login via web está atualmente em pré-visualização. Este recurso é fornecido sem suporte e ainda não é recomendado para uso em ambientes de produção.

Requisitos do sistema

A seguir estão os requisitos do sistema para usar o login via web:

- Virtual Delivery Agent

    - Windows: **sessão única** versão 2607 ou posterior

- Aplicativo Citrix Workspace
    - Windows: versão 2607 ou posterior
- Identidade do host da sessão: Entra unido ou Entra híbrido unido
- Sistema operacional do host da sessão:
    - Windows 11, versão 24H2 com 2025-09 Cumulative Updates for Windows 11 (KB5065789) ou posterior instalado (build 26100.6725)

Como configurar o login via web

O login via web do Citrix está desabilitado por padrão. Para habilitá-lo, siga estas etapas:

1. Conclua a **configuração do Azure e do Microsoft Entra ID** descrita na documentação Microsoft Entra single sign-on. Se você tiver o logon único do Microsoft Entra habilitado em seu ambiente, poderá prosseguir para a próxima etapa.

   As etapas relevantes são:

   a. Registre os aplicativos cliente e de recurso do Citrix.
   b. Habilite o protocolo de autenticação dos Serviços de Área de Trabalho Remota do Microsoft Entra ID para o aplicativo de recurso do Citrix.
   c. Oculte o prompt de consentimento do usuário.
   d. Aprove o aplicativo cliente.
   e. Crie um objeto de servidor Kerberos (somente em ambientes híbridos ingressados no Microsoft Entra).
   f. Revise as políticas de Acesso Condicional do Microsoft Entra.

2. Habilite a configuração de **Logon da Web** em uma política Citrix e aplique a política aos grupos de entrega apropriados.

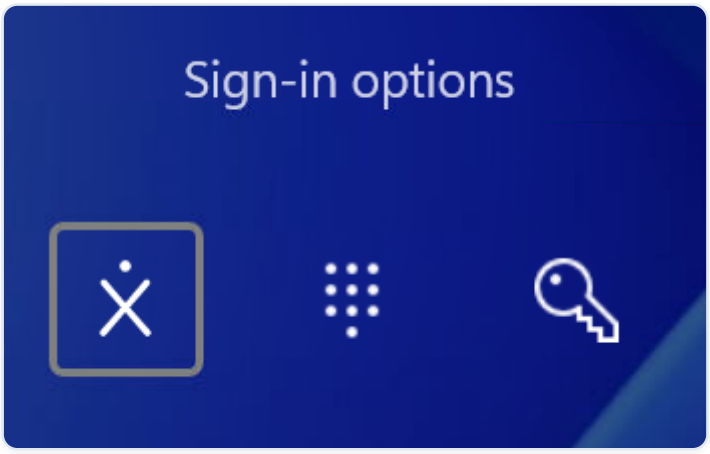
> **NOTA**
>
> - Não é necessário usar o logon único do Microsoft Entra para usar o logon da web.
> - Se a configuração da política ainda não estiver disponível em seu locatário, você pode habilitar o logon da web via registro:

- Chave: HKLM\SOFTWARE\Policies\Citrix\ICAPolicies
- Tipo de valor: DWORD
- Nome do valor: AllowWebSignIn
- Dados do valor: 1

Como usar o login web

Para usar o login web da Citrix para fazer login ou desbloquear sua área de trabalho virtual:

1. Selecione o bloco da Citrix dentre os métodos de logon disponíveis.



2. Clique em **Login Web da Citrix**.



3. Assim que o prompt de autenticação aparecer, autenticar com o método de autenticação necessário.

NOTA

Os métodos de autenticação disponíveis para o usuário são determinados pelo que está habilitado no Microsoft Entra ID.

Configurar locais de recursos

Os locais de recursos contêm os recursos necessários para entregar aplicativos e desktops aos usuários. Você gerencia os recursos a partir do Citrix Cloud. Tipicamente, os recursos incluem:

- Hipervisores ou serviços de nuvem, conhecidos como *hosts*, que incluem:
  - Controladores de domínio do Active Directory.
  - Virtual Delivery Agents (VDAs): Os VDAs são instalados em uma máquina que entrega os aplicativos e desktops aos usuários.
  - Citrix Gateway (opcional): Para habilitar o acesso externo seguro aos aplicativos e desktops oferecidos aos usuários, adicione um dispositivo Citrix Gateway VPX ao local de recursos. Em seguida, configure o Citrix Gateway.
  - Servidores Citrix StoreFront™.
  - Para se comunicar com o Citrix Cloud, cada local de recursos deve conter um Citrix Cloud Connector. Recomenda-se um mínimo de dois Cloud Connectors por local de recursos.

Uma zona é equivalente a um local de recursos. Ao criar um local de recursos e instalar um Cloud Connector, uma zona é criada automaticamente para você. Para mais informações, consulte Zonas.

Para saber mais sobre os tipos de recursos, consulte Conectar ao Citrix Cloud.

Requisitos do host

O hipervisor ou serviço de nuvem, onde você provisiona VMs, precisa de permissões ou configuração exclusivas.

- Se o hipervisor ou serviço de nuvem exigir redes virtuais, siga as orientações em sua documentação.
- Crie a Virtual Private Cloud (VPC) (para AWS ou GCP) ou Virtual Network (VNET) (para Azure) apropriada para as máquinas que você adicionará ao seu local de recursos.

- Crie as regras apropriadas para proteger o tráfego de entrada e saída entre as máquinas na rede virtual. Por exemplo, ao usar o AWS, certifique-se de que o grupo de segurança da VPC tenha as regras apropriadas configuradas para que as máquinas na VPC sejam acessíveis apenas aos endereços IP que você especificar.

Os seguintes tipos de host são suportados:

- Ambientes de virtualização Amazon Web Services (AWS)
- Ambientes de virtualização XenServer®
- Ambientes de virtualização Google Cloud Platform
- Ambientes de virtualização HPE Moonshot
- Ambientes de virtualização Microsoft Azure Resource Manager
- Ambientes de virtualização Microsoft System Center Virtual Machine Manager
- Ambientes de virtualização Nutanix
- Soluções de nuvem e parceiros Nutanix
- Ambientes de virtualização VMware
- Soluções de nuvem e parceiros VMware

Active Directory

Provisione um servidor Windows, instale os Serviços de Domínio Active Directory (AD DS) e promova-o a um Controlador de Domínio. Para obter orientação, consulte a documentação da Microsoft sobre Visão geral dos Serviços de Domínio Active Directory.

As considerações importantes são:

- Você deve ter pelo menos um Controlador de Domínio executando os Serviços de Domínio Active Directory.
- Não instale nenhum componente Citrix em um Controlador de Domínio.

Para obter mais informações, consulte:

- Níveis funcionais do Active Directory
- Gerenciamento de identidade e acesso no Citrix Cloud.
- Conectar o Active Directory ao Citrix Cloud
- Cenários de implantação para usar o Connector Appliance com o Active Directory

Cloud Connectors

O Cloud Connector é um grupo de serviços do Citrix Cloud que permite a comunicação entre os VDAs, o StoreFront e o Delivery Controller baseado em nuvem. Você pode instalar os Cloud Connectors interativamente ou pela linha de comando.

Para obter mais informações sobre os Cloud Connectors, consulte:

- Citrix Cloud Connector
- Detalhes técnicos
- Configuração de proxy e firewall
- Instalação
- Atualizações do Connector

Considerações de tamanho e escala

- Ao avaliar o Citrix DaaS™ para dimensionamento e escalabilidade, considere todos os componentes.
- Pesquise e teste a configuração dos Cloud Connectors e do StoreFront para seus requisitos específicos.
- Dimensionar as máquinas de forma insuficiente pode impactar negativamente o desempenho do sistema.

O artigo Considerações de tamanho e escala para Cloud Connectors inclui:

- Informações de teste de tamanho e escala
- Capacidades máximas testadas
- Recomendações de melhores práticas para a configuração da máquina do Cloud Connector

Adicionar um tipo de recurso

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **Locais de Recursos**.
3. Selecione **+ Locais de Recursos** para adicionar um local de recurso.
4. Insira um nome para o local de recurso e clique em **Salvar**. Para obter informações sobre considerações de nomenclatura, consulte Restrições de nome.
5. Sob o novo local de recurso, selecione **+ Cloud Connectors**.

6. Baixe e instale o software Cloud Connector em pelo menos dois servidores no domínio onde você tem seus recursos do Citrix DaaS.
   - Durante a instalação, selecione o local de recurso que você criou nas etapas anteriores.
   - Após a instalação, o Citrix Cloud adiciona os servidores ao local do recurso e registra os domínios nos quais você instalou os Cloud Connectors.
7. Verifique se os domínios registrados estão ativos:
   - No menu do Citrix Cloud, selecione **Gerenciamento de Acesso de Identidade**.
   - Selecione **Domínios**. Uma lista de domínios onde os Cloud Connectors foram implantados é exibida.
   - Localize os domínios que você está usando com o Citrix DaaS. Os domínios ativos são exibidos com uma barra verde no lado esquerdo da entrada do domínio.

   Se o seu domínio não tiver o indicador visual, o domínio estará em um estado **não utilizado**. Se você especificar um domínio não utilizado durante a configuração do catálogo de máquinas, a criação do catálogo falhará. Para garantir que a configuração do catálogo de máquinas ocorra sem erros, siga as etapas em Ativar um domínio não utilizado.

   Para obter mais informações, consulte CTX473009: Assistente de Criação de Catálogo DaaS: "Erro Interno do Servidor" ao criar novas contas de máquina.

Ativar um domínio não utilizado

1. Na guia **Domínio**, em **Gerenciamento de Identidade e Acesso**, selecione **Mostrar Domínios Não Utilizados**. Depois de selecionar esta opção, o rótulo muda para **Ocultar Domínios Não Utilizados**.
2. Localize o domínio não utilizado na lista. Os domínios não utilizados exibem uma barra cinza no lado esquerdo da entrada do domínio e um menu de reticências de opção única no lado direito.
3. Selecione o menu de reticências e, em seguida, selecione **Usar domínio**. A barra cinza fica verde e o menu de reticências muda para **Desativar**.

Onde ir em seguida

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina designada para entregar aplicativos ou um desktop aos seus usuários.
- Para configurar o local do recurso para tipos de host específicos:

- Ambientes de virtualização AWS
- Ambientes de virtualização do Google Cloud
- Ambientes de virtualização HPE Moonshot
- Ambientes de virtualização do Microsoft Azure Resource Manager
- Ambientes de virtualização do Microsoft System Center Virtual Machine Manager
- Ambientes de virtualização Nutanix
- Soluções de nuvem e parceiros Nutanix
- Ambientes de virtualização VMware
- Soluções de nuvem e parceiros VMware
- Ambientes de virtualização XenServer

- Para uma implantação completa, Crie e gerencie conexões e recursos para um local de recurso.
- Revise todas as etapas do processo de instalação e configuração

Ambientes de virtualização Amulet Hotkey CoreStation

O Citrix DaaS™ gerencia suas cargas de trabalho do Amulet Hotkey CoreStation por meio de um plug-in do Amulet Hotkey CoreStation gerenciado pela Citrix, presente no plano de controle do DaaS. Com este plug-in, você pode criar conexões com seu gabinete Amulet Hotkey CoreStation, criar catálogos e gerenciar o consumo de energia das máquinas no catálogo.

Etapas principais

1. Configure seu ambiente Amulet Hotkey CoreStation.
2. Crie uma conexão com o gabinete Amulet Hotkey CoreStation.
3. Crie um catálogo de máquinas.

> **Nota:**
>
> Antes de criar um catálogo, certifique-se de ter um ou mais nós Amulet Hotkey CoreStation e instale VDAs nesses nós. Você pode considerar o gabinete Amulet Hotkey CoreStation como o hipervisor e os nós como VMs.

4. Crie um grupo de entrega.

Próximos passos

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que entregará aplicativos ou uma área de trabalho aos seus usuários.
- Para criar e gerenciar conexões, consulte Conexão com o Amulet Hotkey CoreStation.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização AWS

Este artigo descreve como configurar sua conta AWS como um local de recurso que você pode usar com o Citrix DaaS. O local do recurso é usado para provisionar cargas de trabalho no AWS EC2 e em instâncias gerenciadas do Amazon WorkSpaces Core. Para obter a lista de tipos de SO compatíveis com as instâncias gerenciadas do Amazon WorkSpaces Core, consulte VDAs em instâncias gerenciadas do Amazon WorkSpaces Core.

Comparação de diferentes locais de recursos configuráveis: MCS para AWS EC2, MCS para instâncias gerenciadas do Amazon WorkSpaces Core e Implantação Rápida para pacotes do Amazon WorkSpaces Core.

MCS PARA AWS EC2	MCS PARA INSTÂNCIAS GERENCIADAS DO AMAZON WORKSPACES CORE	IMPLANTAÇÃO RÁPIDA PARA PACOTES DO AMAZON WORKSPACES CORE
A Citrix® lida com o provisionamento de VMs em sua conta AWS	A Citrix lida com o provisionamento de VMs em sua conta AWS	A Amazon lida com o provisionamento de VMs na conta WorkSpaces gerenciada pela AWS
Fluxo de trabalho MCS avançado para gerenciamento do ciclo de vida da VM	Fluxo de trabalho MCS avançado para gerenciamento do ciclo de vida da VM	Fluxo de trabalho rápido e fácil de 5 etapas
Instâncias EC2	Instâncias gerenciadas do WorkSpaces Core (utilizam instâncias EC2 sob demanda	Pacotes do WorkSpaces, capacidade totalmente

MCS PARA AWS EC2	MCS PARA INSTÂNCIAS GERENCIADAS DO AMAZON WORKSPACES CORE	IMPLANTAÇÃO RÁPIDA PARA PACOTES DO AMAZON WORKSPACES CORE
	lançadas diretamente em sua conta AWS)	gerenciada pela AWS (abstração de nível superior)
Sem suporte para licenciamento do Microsoft 365	Suporte BYOL para Microsoft 365	Suporte BYOL para Microsoft 365
Windows Server, Windows Desktop e Linux	Windows Server, Windows Desktop e Linux	Windows Server, Windows Desktop
VMs persistentes e não persistentes	VMs persistentes e não persistentes	Somente VMs persistentes
Somente pagamento conforme o uso	Pagamento conforme o uso	Somente preço fixo por mês
Citrix DaaS e Citrix Virtual Apps and Desktops™	Citrix DaaS e Citrix Virtual Apps and Desktops™	Somente Citrix DaaS

O local de recurso inclui um conjunto básico de componentes, ideal para uma prova de conceito, ou outra implantação que não exija recursos espalhados por várias zonas de disponibilidade.

Ao concluir as tarefas neste artigo, seu local de recurso inclui os seguintes componentes:

- Uma nuvem privada virtual (VPC) com sub-redes públicas e privadas dentro de uma única zona de disponibilidade.
- Uma instância que funciona como um Controlador de Domínio do Active Directory e servidor DNS, localizada na sub-rede privada da VPC.
- Duas instâncias unidas ao domínio nas quais o Citrix Cloud Connector™ está instalado, localizadas na sub-rede privada da VPC.
- Uma instância que atua como um host bastion, localizada na sub-rede pública da sua VPC. Esta instância é usada para iniciar conexões RDP com as instâncias na sub-rede privada para fins de administração. Depois de concluir a configuração do seu local de recurso, você pode desligar esta instância para que ela não seja mais facilmente acessível. Quando você precisar gerenciar outras instâncias na sub-rede privada, como instâncias VDA, você pode reiniciar a instância do host bastion.

Depois de concluir as tarefas, você pode instalar VDAs, provisionar máquinas, criar catálogos de máquinas e criar Grupos de Entrega.

Visão geral da tarefa

Configurar uma nuvem privada virtual (VPC) com sub-redes públicas e privadas. Ao concluir esta tarefa, a AWS implanta gateways NAT com um endereço IP Elástico na sub-rede pública. Isso permite que as instâncias na sub-rede privada acessem a Internet. As instâncias na sub-rede pública são acessíveis ao tráfego público de entrada, enquanto as instâncias na sub-rede privada não são.

Configurar grupos de segurança. Os grupos de segurança atuam como firewalls virtuais que controlam o tráfego para as instâncias em sua VPC. Você adiciona regras aos seus grupos de segurança que permitem que as instâncias em sua sub-rede pública se comuniquem com as instâncias em sua sub-rede privada. Você também associa esses grupos de segurança a cada instância em sua VPC.

Criar um conjunto de opções DHCP. Os serviços Amazon VPC, DHCP e DNS são fornecidos por padrão, o que afeta como você configura o DNS em seu Controlador de Domínio do Active Directory. O DHCP da Amazon não pode ser desativado e o DNS da Amazon pode ser usado apenas para resolução de DNS público, não para resolução de nomes do Active Directory. Para especificar o domínio e os servidores de nomes entregues às instâncias via DHCP, crie um conjunto de opções DHCP. O conjunto atribui o sufixo de domínio do Active Directory e especifica o servidor DNS para todas as instâncias em sua VPC. Para garantir que os registros Host (A) e Reverse Lookup (PTR) sejam registrados automaticamente quando as instâncias ingressarem no domínio, você configura as propriedades do adaptador de rede para cada instância que você adicionar à sub-rede privada.

Adicionar um host bastion, Controlador de Domínio e Cloud Connectors à VPC. Através do host bastion, você pode fazer logon em instâncias na sub-rede privada para configurar o domínio, unir instâncias ao domínio e instalar o Cloud Connector.

Tarefa 1: Configurar a VPC

1. No console de gerenciamento da AWS, selecione **VPC**.
2. No Painel da VPC, selecione **Criar VPC**.
3. Selecione **VPC e mais**.
4. Em NAT gateways ($), selecione **Em 1 AZ** ou **1 por AZ**.
5. Em opções de DNS, deixe **Habilitar nomes de host DNS** selecionado.

6. Selecione **Criar VPC**. A AWS cria as sub-redes públicas e privadas, o gateway de Internet, as tabelas de rotas e o grupo de segurança padrão.

> **Observação:**
>
> Alterar o nome de uma Nuvem Privada Virtual (VPC) da AWS no console da AWS quebra a unidade de hospedagem existente no Citrix Cloud. Quando a unidade de hospedagem está quebrada, você não pode criar catálogos ou adicionar máquinas a catálogos existentes. De Problema Conhecido: PMCS-7701

Tarefa 2: Configurar grupos de segurança

Esta tarefa cria e configura os seguintes grupos de segurança para sua VPC:

- Um grupo de segurança público para associar às instâncias em sua sub-rede pública.
- Um grupo de segurança privado para associar às instâncias em sua sub-rede privada.

Para criar os grupos de segurança:

1. No Painel da VPC, selecione **Grupos de Segurança**.
2. Crie um grupo de segurança para o grupo de segurança público. Selecione **Criar Grupo de Segurança** e insira uma tag de nome e uma descrição para o grupo. Em VPC, selecione a VPC que você criou anteriormente. Selecione **Sim, Criar**.

Configurar o grupo de segurança público

1. Na lista de grupos de segurança, selecione o grupo de segurança público.
2. Selecione a guia **Regras de entrada** e selecione Editar para criar as seguintes regras:

TIPO	ORIGEM
Todo o Tráfego	Selecione o grupo de segurança Privado.
Todo o Tráfego	Selecione o grupo de segurança Público.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0

TIPO	ORIGEM
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Confiabilidade da Sessão)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. Quando terminar, selecione **Salvar**.
4. Selecione a guia **Regras de Saída** e selecione **Editar** para criar as seguintes regras.

TIPO	DESTINO
TODO o Tráfego	0.0.0.0/0

5. Quando terminar, selecione **Salvar**.

Configurar o grupo de segurança privado

1. Na lista de grupos de segurança, selecione o grupo de segurança Privado.
2. Se você ainda não configurou o tráfego do grupo de segurança público, você deve definir as portas TCP. Selecione a guia **Inbound Rules** e selecione **Edit** para criar as seguintes regras:

TIPO	ORIGEM
ICMP	Selecione o grupo de segurança Público.
TCP 53 (DNS)	Selecione o grupo de segurança Público.
UDP 53 (DNS)	Selecione o grupo de segurança Público.
80 (HTTP)	Selecione o grupo de segurança Público.
TCP 135	Selecione o grupo de segurança Público.
TCP 389	Selecione o grupo de segurança Público.
UDP 389	Selecione o grupo de segurança Público.
443 (HTTPS)	Selecione o grupo de segurança Público.

TIPO	ORIGEM
TCP 1494 (ICA/HDX)	Selecione o grupo de segurança Público.
TCP 2598 (Confiabilidade da Sessão)	Selecione o grupo de segurança Público.
3389 (RDP)	Selecione o grupo de segurança Público.
TCP 49152–65535	Selecione o grupo de segurança Público.

3. Quando terminar, selecione **Salvar.**
4. Selecione a guia **Regras de Saída** e selecione **Editar** para criar as seguintes regras.

TIPO	DESTINO
TODO o Tráfego	Selecione o grupo de segurança Privado.
TODO o Tráfego	0.0.0.0/0

5. Quando terminar, selecione **Salvar**.

Tarefa 3: Iniciar instâncias

Execute as seguintes etapas para criar quatro instâncias EC2 e descriptografar a senha de Administrador padrão que a Amazon gera:

1. No console de gerenciamento da AWS, selecione **EC2**.
2. No Painel do EC2, selecione **Iniciar Instância**.
3. Selecione uma imagem de máquina do Windows Server e o tipo de instância.
4. Na página **Configurar Detalhes da Instância**, insira um nome para a instância e selecione a VPC que você configurou anteriormente.
5. Em **Sub-rede**, faça as seguintes seleções para cada instância:
    - Host bastion: Selecione a sub-rede Pública
    - Controlador de domínio e Conectores: Selecione a sub-rede Privada
6. Em **Atribuir automaticamente endereço IP público**, faça as seguintes seleções para cada instância:
    - Host bastion: Selecione **Habilitar**

- Controlador de domínio e conectores: Selecione **Usar configuração padrão** ou **Desabilitar**

7. Em **Interfaces de Rede**, insira um endereço IP primário dentro do intervalo de IP da sua sub-rede privada para as instâncias do Controlador de Domínio e do Cloud Connector.
8. Se necessário, na página **Adicionar Armazenamento**, modifique o tamanho do disco.
9. Na página **Marcar Instância**, insira um nome amigável para cada instância.
10. Na página **Configurar Grupos de Segurança**, selecione **Selecionar um grupo de segurança existente** e, em seguida, faça as seguintes seleções para cada instância:
    - Host bastion: Selecione o grupo de segurança Público.
    - Controlador de domínio e Cloud Connectors: Selecione o grupo de segurança Privado.
11. Revise suas seleções e, em seguida, selecione **Iniciar**.
12. Crie um novo par de chaves ou selecione um existente. Se você criar um novo par de chaves, baixe seu arquivo de chave privada (`.pem`) e mantenha-o em um local seguro. Você deve fornecer sua chave privada ao adquirir a senha de Administrador padrão para a instância.
13. Selecione **Iniciar Instâncias**. Selecione **Visualizar Instâncias** para exibir uma lista de suas instâncias. Aguarde até que a instância recém-iniciada tenha passado por todas as verificações de status antes de acessá-la.
14. Adquira a senha de Administrador padrão para cada instância.
    a. Na lista de instâncias, selecione a instância e, em seguida, selecione **Conectar**.
    b. Vá para a guia **Cliente RDP**, selecione **Obter Senha** e carregue seu arquivo de chave privada (`.pem`) quando solicitado.
    c. Selecione **Descriptografar Senha** para obter a senha legível. A AWS exibe a senha padrão.
15. Repita todos os passos a partir do passo 2 até que você tenha criado quatro instâncias:
    - Uma instância de host bastion em sua sub-rede pública
    - Três instâncias em sua sub-rede privada para serem usadas como:
        - Uma como Controlador de Domínio
        - Duas como Cloud Connectors

Tarefa 4: Criar um conjunto de opções DHCP

1. No Painel da VPC, selecione **Conjuntos de Opções DHCP**.
2. Insira as seguintes informações:
    - Tag de nome: Insira um nome amigável para o conjunto.
    - Nome de domínio: Insira o nome de domínio totalmente qualificado que você usa ao configurar a instância do Controlador de Domínio.
    - Servidores de nome de domínio: Insira o endereço IP privado que você atribuiu à instância do Controlador de Domínio e a string **AmazonProvidedDNS**, separados por vírgulas.
    - Servidores NTP: Deixe este campo em branco.
    - Servidores de nome NetBIOS: Insira o endereço IP privado da instância do Controlador de Domínio.
    - Tipo de nó NetBIOS: Insira **2**.
3. Selecione **Sim, Criar.**
4. Associe o novo conjunto à sua VPC:
    a. No Painel da VPC, selecione **Suas VPCs** e, em seguida, selecione a VPC que você configurou anteriormente.
    b. Selecione **Ações > Editar Conjunto de Opções DHCP**.
    c. Quando solicitado, selecione o novo conjunto que você criou e, em seguida, selecione **Salvar**.

Tarefa 5: Configurar as instâncias

1. Usando um cliente RDP, conecte-se ao endereço IP público da instância do host bastion. Quando solicitado, insira as credenciais da conta de Administrador.
2. Na instância do host bastion, inicie **Conexão de Área de Trabalho Remota** e conecte-se ao endereço IP privado da instância que você deseja configurar. Quando solicitado, insira as credenciais de Administrador da instância.
3. Para todas as instâncias na sub-rede privada, configure as configurações de DNS:
    a. Selecione **Iniciar > Painel de Controle > Rede e Internet > Central de Rede e Compartilhamento > Alterar configurações do adaptador**. Clique duas vezes na conexão de rede exibida.
    b. Selecione **Propriedades > Protocolo de Internet Versão 4 (TCP/IPv4) > Propriedades**.

c. Selecione **Avançado > DNS**. Certifique-se de que as seguintes configurações estejam habilitadas e, em seguida, selecione **OK**:

- **Registrar os endereços desta conexão no DNS**
- **Usar o sufixo DNS desta conexão no registro DNS**

4. Configure o Controlador de Domínio:

a. Usando o Gerenciador de Servidores, adicione a função Serviços de Domínio Active Directory com todos os recursos padrão.

b. Promova a instância a um Controlador de Domínio. Durante a promoção, habilite o DNS e use o nome de domínio que você especificou ao criar o conjunto de opções DHCP. Reinicie a instância quando solicitado.

5. Configure o primeiro Cloud Connector:

a. Una a instância ao domínio e reinicie quando solicitado. A partir da instância do host bastion, reconecte-se à instância usando RDP.

b. Faça login no Citrix Cloud. Selecione **Locais de Recursos** no menu superior esquerdo.

c. Baixe o Cloud Connector.

d. Quando solicitado, execute o arquivo `cwcconnector.exe` e forneça suas credenciais do Citrix Cloud. Siga o assistente.

e. Após a conclusão, selecione **Atualizar** para exibir a página **Locais de Recursos**. Quando o Cloud Connector estiver registrado, a instância aparecerá na página.

6. Repita as etapas para configurar o Cloud Connector para configurar o segundo Cloud Connector.

7. Anexe uma Política IAM aos Cloud Connectors para oferecer suporte a conexões de hospedagem AWS com autorização baseada em função. Você deve ter a mesma Política IAM anexada a todos os Cloud Connectors em um local de recurso. Para obter informações sobre permissões AWS, consulte Permissões AWS necessárias - Amazon EC2 e Permissões AWS necessárias - Instâncias Gerenciadas do Amazon WorkSpaces Core.

Onde ir em seguida

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina designada para entregar aplicativos ou um desktop aos seus usuários.
- Para criar e gerenciar conexões, consulte:

    - Conexão com AWS
    - Conexão com Instâncias Gerenciadas do Amazon WorkSpaces Core
- Revise todas as etapas do processo de instalação e configuração

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização do Google Cloud

O Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™) permite provisionar e gerenciar máquinas no Google Cloud.

Pré-requisitos

Antes de começar a provisionar as VMs para o Google Cloud Platform (GCP), você deve garantir que os seguintes pré-requisitos sejam atendidos.

1. A assinatura Citrix deve incluir suporte para cargas de trabalho Hybrid Multi-Cloud. Para obter mais informações, consulte Comparar recursos de assinatura Citrix.
2. A conta de administrador deve ter permissões suficientes para criar conexões de host, catálogos de máquinas e grupos de entrega. Para obter mais informações, consulte Configurar Administração Delegada.
3. Identifique um projeto do Google Cloud, no qual todos os recursos de computação associados ao catálogo de máquinas são armazenados. Pode ser um projeto existente ou um novo. Para obter mais informações, consulte Projetos do Google Cloud.
4. Habilite as APIs do Google Cloud necessárias para a integração com o Citrix DaaS. Para obter mais informações, consulte Habilitar APIs do Google Cloud.
5. Crie as contas de serviço no Google Cloud e conceda as permissões apropriadas. Para obter mais informações, consulte Configurar e atualizar contas de serviço.
6. Baixe o arquivo de chave para a Conta de Serviço do Citrix Cloud. Para obter mais informações, consulte Chave da Conta de Serviço do Citrix Cloud.
7. As máquinas virtuais devem ter acesso às APIs do Google sem um endereço IP público. Para obter mais informações, consulte Habilitar Acesso Privado do Google.

Projetos do Google Cloud

Existem basicamente dois tipos de projetos do Google Cloud:

- Projeto de provisionamento: Neste caso, a conta de administrador atual é proprietária das máquinas provisionadas no projeto. Este projeto também é conhecido como projeto local.
- Projeto VPC Compartilhada: Projeto no qual as máquinas criadas no projeto de provisionamento usam a VPC do projeto VPC Compartilhada. A conta de administrador usada para provisionar projetos tem permissões limitadas neste projeto, especificamente, apenas permissões para usar a VPC.

URLs de endpoint de serviço

Você deve ter acesso às seguintes URLs:

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Habilitar APIs do Google Cloud

Para usar a funcionalidade do Google Cloud por meio do Studio, habilite estas APIs em seu projeto do Google Cloud:

- Compute Engine API
- Cloud Resource Manager API
- API de Gerenciamento de Identidade e Acesso (IAM)
- Cloud Build API

No console do Google Cloud, conclua estas etapas:

1. No menu superior esquerdo, selecione **APIs e serviços > APIs e serviços ativados**.
2. Na tela **APIs e serviços ativados**, certifique-se de que a API do Compute Engine esteja ativada. Caso contrário, siga estas etapas:
    a. navegar para **APIs and Services > Library**.
    b. Na caixa de pesquisa, digite *Compute Engine*.
    c. Nos resultados da pesquisa, selecione **Compute Engine API**.
    d. Na página **Compute Engine API**, selecione **Enable**.
3. Ative a API do Cloud Resource Manager.

a. navegar para **APIs and Services > Library**.

b. Na caixa de pesquisa, digite *Cloud Resource Manager*.

c. Nos resultados da pesquisa, selecione **Cloud Resource Manager API**.

d. Na página **Cloud Resource Manager API**, selecione **Enable**. O status da API é exibido.

4. Da mesma forma, ative a **API Identity and Access Management (IAM)** e a **API Cloud Build**, e a **API Cloud Key Management Service (KMS)**.

Você também pode usar o Google Cloud Shell para ativar as APIs. Para fazer isso:

1. Abra o Google Console e carregue o Cloud Shell.
2. Execute os quatro comandos a seguir no Cloud Shell:
   - gcloud services enable compute.googleapis.com.
   - gcloud serviços habilitar cloudresourcemanager.googleapis.com
   - gcloud serviços habilitar iam.googleapis.com
   - gcloud serviços habilitar cloudbuild.googleapis.com
   - gcloud serviços habilitar cloudkms.googleapis.com
3. Clique em **Autorizar** quando o Cloud Shell solicitar.

Configurar e atualizar contas de serviço

> **Nota:**
>
> O GCP está introduzindo mudanças no comportamento padrão do Serviço Cloud Build e no uso de contas de serviço após April 29, 2024. Para obter mais informações, consulte Alteração da Conta de Serviço do Cloud Build. Seus projetos Google existentes com a API Cloud Build habilitada antes de April 29, 2024 não são afetados por esta mudança. No entanto, se você quiser manter o comportamento existente do Serviço Cloud Build após April 29, você pode criar ou aplicar a política da organização para desabilitar a imposição da restrição antes de habilitar a API Cloud Build. Como resultado, o conteúdo a seguir é dividido em dois: Antes de April 29, 2024 e Depois de April 29, 2024. Se você definir a nova política da organização, siga a seção Antes de April 29, 2024.

Antes de April 29, 2024

O Citrix Cloud™ usa três contas de serviço separadas dentro do projeto Google Cloud:

- *Conta de Serviço do Citrix Cloud*: Esta conta de serviço permite que o Citrix Cloud acesse o projeto Google, provisione e gerencie máquinas. Esta conta de serviço se autentica no Google Cloud usando uma chave gerada pelo Google Cloud.

  Você deve criar esta conta de serviço manualmente, conforme descrito aqui. Para obter mais informações, consulte Criar uma Conta de Serviço do Citrix Cloud.

  Você pode identificar esta conta de serviço com um endereço de e-mail. Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Conta de Serviço do Cloud Build*: Esta conta de serviço é provisionada automaticamente depois que você habilita todas as APIs mencionadas em Habilitar APIs do Google Cloud. Para visualizar todas as contas de serviço criadas automaticamente, navegar para **IAM e Administrador > IAM** no console do **Google Cloud** e selecione a caixa de seleção **Incluir concessões de função fornecidas pelo Google**.

  Você pode identificar esta conta de serviço por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **cloudbuild**. Por exemplo, `<project-id>@cloudbuild.gserviceaccount.com`

  Verifique se a conta de serviço recebeu as seguintes funções. Se você precisar adicionar funções, siga as etapas descritas em Adicionar funções à conta de serviço do Cloud Build.

  - Conta de Serviço do Cloud Build
  - Administrador de Instância de Computação
  - Usuário da Conta de Serviço

- *Conta de Serviço do Cloud Compute*: Esta conta de serviço é adicionada pelo Google Cloud às instâncias criadas no Google Cloud assim que a API Compute é ativada. Esta conta tem a função de editor básico do IAM para realizar as operações. No entanto, se você excluir a permissão padrão para ter um controle mais granular, deverá adicionar uma função de **Administrador de Armazenamento** que requer as seguintes permissões:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

Você pode identificar esta conta de serviço por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**. Por exemplo, `<project-id>-compute@developer.gserviceaccount.com`.

CRIAR UMA CONTA DE SERVIÇO DO CITRIX CLOUD

Para criar uma Conta de Serviço do Citrix Cloud, siga estas etapas:

1. No console do Google Cloud, navegar para **IAM e Administrador > Contas de serviço**.
2. Na página **Contas de serviço**, selecione **CRIAR CONTA DE SERVIÇO**.
3. Na página **Criar conta de serviço**, insira as informações necessárias e, em seguida, selecione **CRIAR E CONTINUAR**.
4. Na página **Conceder a esta conta de serviço acesso ao projeto**, clique no menu suspenso **Selecionar uma função** e selecione as funções necessárias. Clique em **+ADICIONAR OUTRA FUNÇÃO** se quiser adicionar mais funções.

   Cada conta (pessoal ou de serviço) tem várias funções que definem o gerenciamento do projeto. Conceda as seguintes funções a esta conta de serviço:

   - Compute Admin
   - Storage Admin
   - Cloud Build Editor
   - Service Account User
   - Cloud Datastore User
   - Cloud KMS Crypto Operator

   O Cloud KMS Crypto Operator requer as seguintes permissões:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list
   - cloudkms.cryptoKeyVersions.useToDecrypt
   - cloudkms.cryptoKeyVersions.useToEncrypt

> **Observação:**

> Habilite todas as APIs para obter a lista completa de funções disponíveis ao criar uma nova conta de serviço.

5. Clique em **CONTINUAR**
6. Na página **Conceder acesso de usuários a esta conta de serviço**, adicione usuários ou grupos para conceder-lhes acesso para realizar ações nesta conta de serviço.
7. Clique em **CONCLUÍDO**.
8. navegar para o console principal do IAM.
9. Identifique a conta de serviço criada.
10. Valide se as funções foram atribuídas com sucesso.

Considerações:

Ao criar a conta de serviço, considere o seguinte:

- As etapas **Conceder a esta conta de serviço acesso ao projeto** e **Conceder acesso de usuários a esta conta de serviço** são opcionais. Se você optar por pular essas etapas de configuração opcionais, a conta de serviço recém-criada não será exibida na página **IAM e Administrador > IAM**.
- Para exibir as funções associadas a uma conta de serviço, adicione as funções sem pular as etapas opcionais. Esse processo garante que as funções apareçam para a conta de serviço configurada.

CHAVE DA CONTA DE SERVIÇO DO CITRIX CLOUD

A chave da conta de serviço do Citrix Cloud é necessária para criar uma conexão no Citrix DaaS. A chave está contida em um arquivo de credenciais (.json). O arquivo é baixado e salvo automaticamente na pasta **Downloads** depois que você cria a chave. Ao criar a chave, certifique-se de definir o tipo de chave como JSON. Caso contrário, o Studio não poderá analisá-la.

Para criar uma chave de conta de serviço, navegar para **IAM e Administrador > Contas de serviço** e clique no endereço de e-mail da conta de serviço do Citrix Cloud. Mude para a guia **Chaves** e selecione **Adicionar chave > Criar nova chave**. Certifique-se de selecionar **JSON** como o tipo de chave.

> **Dica:**

> Crie chaves usando a página **Contas de serviço** no console do Google Cloud. Recomendamos que você altere as chaves regularmente por motivos de segurança. Você pode fornecer novas chaves para o aplicativo Citrix Virtual Apps and Desktops editando uma conexão existente do Google Cloud.

ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CITRIX CLOUD

Para adicionar funções à conta de serviço do Citrix Cloud:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM > PERMISSÕES**, localize a conta de serviço que você criou, identificável por um endereço de e-mail.

   Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Selecione o ícone de lápis para editar o acesso ao principal da conta de serviço.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço uma a uma e, em seguida, selecione **SALVAR**.

ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CLOUD BUILD

Para adicionar funções à conta de serviço do Cloud Build:

1. No console do Google Cloud, navegar até **IAM e administrador > IAM**.
2. Na página **IAM**, localize a conta de serviço do Cloud Build, identificável por um endereço de e-mail que começa com o **ID do projeto** e a palavra **cloudbuild**.

   Por exemplo, `<project-id>@cloudbuild.gserviceaccount.com`
3. Selecione o ícone de lápis para editar as funções da conta do Cloud Build.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço do Cloud Build uma por uma e, em seguida, selecione **SALVAR**.

> **Nota:**
>
> Habilite todas as APIs para obter a lista completa de funções.

Após April 29, 2024

O Citrix Cloud usa duas contas de serviço separadas dentro do projeto do Google Cloud:

- *Conta de Serviço do Citrix Cloud*: Esta conta de serviço permite que o Citrix Cloud acesse o projeto do Google, provisione e gerencie máquinas. Esta conta de serviço se autentica no Google Cloud usando uma chave gerada pelo Google Cloud.

  Você deve criar esta conta de serviço manualmente.

  Você pode identificar esta conta de serviço por um endereço de e-mail. Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Conta de Serviço do Cloud Compute*: Esta conta de serviço é provisionada automaticamente depois que você habilita todas as APIs mencionadas em Habilitar APIs do Google Cloud. Para visualizar todas as contas de serviço criadas automaticamente, navegar para **IAM e Admin > IAM** no console do **Google Cloud** e selecione a caixa de seleção **Incluir concessões de função fornecidas pelo Google**. Esta conta tem a função de editor básico do IAM para realizar as operações. No entanto, se você excluir a permissão padrão para ter um controle mais granular, deverá adicionar a função de **Administrador de Armazenamento** que requer as seguintes permissões:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

  Você pode identificar esta conta de serviço por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**. Por exemplo, `<project-id>-compute@developer.gserviceaccount.com.`.

  Verifique se a conta de serviço recebeu as seguintes funções.

  - Conta de Serviço do Cloud Build
  - Administrador de Instância de Computação
  - Usuário da Conta de Serviço

CRIAR UMA CONTA DE SERVIÇO DO CITRIX CLOUD

Para criar uma Conta de Serviço do Citrix Cloud, siga estas etapas:

1. No console do Google Cloud, navegar para **IAM e Administrador > Contas de serviço**.

2. Na página **Contas de serviço**, selecione **CRIAR CONTA DE SERVIÇO**.
3. Na página **Criar conta de serviço**, insira as informações necessárias e, em seguida, selecione **CRIAR E CONTINUAR**.
4. Na página **Conceder a esta conta de serviço acesso ao projeto**, clique no menu suspenso **Selecionar um papel** e selecione os papéis necessários. Clique em **+ADICIONAR OUTRO PAPEL** se quiser adicionar mais papéis.

   Cada conta (pessoal ou de serviço) tem vários papéis que definem o gerenciamento do projeto. Conceda os seguintes papéis a esta conta de serviço:

   - Administrador de Computação
   - Administrador de Armazenamento
   - Editor do Cloud Build
   - Usuário da Conta de Serviço
   - Usuário do Cloud Datastore
   - Cloud KMS Crypto Operator

   O Operador de Criptografia do Cloud KMS requer as seguintes permissões:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

   > **Nota:**
   >
   > Habilite todas as APIs para obter a lista completa de funções disponíveis ao criar uma nova conta de serviço.

5. Clique em **CONTINUAR**
6. Na página **Conceder acesso de usuários a esta conta de serviço**, adicione usuários ou grupos para conceder a eles acesso para realizar ações nesta conta de serviço.
7. Clique em **CONCLUÍDO**.
8. navegar para o console principal do IAM.
9. Identifique a conta de serviço criada.

10. Valide se as funções foram atribuídas com sucesso.

Considerações:

Ao criar a conta de serviço, considere o seguinte:

- As etapas **Conceder a esta conta de serviço acesso ao projeto** e **Conceder aos usuários acesso a esta conta de serviço** são opcionais. Se você optar por pular essas etapas de configuração opcionais, a conta de serviço recém-criada não será exibida na página **IAM e Administração > IAM**.
- Para exibir as funções associadas a uma conta de serviço, adicione as funções sem pular as etapas opcionais. Esse processo garante que as funções apareçam para a conta de serviço configurada.

CHAVE DA CONTA DE SERVIÇO DO CITRIX CLOUD

A chave da conta de serviço do Citrix Cloud é necessária para criar uma conexão no Citrix DaaS. A chave está contida em um arquivo de credenciais (.json). O arquivo é baixado e salvo automaticamente na pasta **Downloads** depois que você cria a chave. Ao criar a chave, certifique-se de definir o tipo de chave como JSON. Caso contrário, o Studio não poderá analisá-la.

Para criar uma Chave de Conta de Serviço, navegar para **IAM e Administração > Contas de serviço** e clique no endereço de e-mail da Conta de Serviço do Citrix Cloud. Mude para a guia **Chaves** e selecione **Adicionar Chave > Criar nova chave**. Certifique-se de selecionar **JSON** como o tipo de chave.

> **Dica:**
>
> Crie chaves usando a página **Contas de serviço** no console do Google Cloud. Recomendamos que você altere as chaves regularmente por motivos de segurança. Você pode fornecer novas chaves para o aplicativo Citrix Virtual Apps and Desktops editando uma conexão existente do Google Cloud.

ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CITRIX CLOUD

Para adicionar funções à conta de serviço do Citrix Cloud:

1. No console do Google Cloud, navegar para **IAM e Administração > IAM**.
2. Na página **IAM > PERMISSÕES**, localize a conta de serviço que você criou, identificável por um endereço de e-mail.

Por exemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`

3. Selecione o ícone de lápis para editar o acesso ao principal da conta de serviço.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço uma a uma e, em seguida, selecione **SALVAR**.

ADICIONAR FUNÇÕES À CONTA DE SERVIÇO DO CLOUD COMPUTE

Para adicionar funções à Conta de Serviço do Cloud Compute:

1. No console do Google Cloud, navegar para **IAM e Administrador > IAM**.
2. Na página **IAM**, localize a Conta de Serviço do Cloud Compute, identificável por um endereço de e-mail que começa com o **ID do Projeto** e a palavra **compute**.

   Por exemplo, `<project-id>-compute@developer.gserviceaccount.com`
3. Selecione o ícone de lápis para editar as funções da conta do Cloud Build.
4. Na página **Editar acesso a "project-id"** para a opção principal selecionada, selecione **ADICIONAR OUTRA FUNÇÃO** para adicionar as funções necessárias à sua conta de serviço do Cloud Build uma a uma e, em seguida, selecione **SALVAR**.

> **Nota:**
>
> Habilite todas as APIs para obter a lista completa de funções.

Permissões de armazenamento e gerenciamento de bucket

O Citrix DaaS melhora o processo de relatório de falhas de compilação na nuvem para o serviço Google Cloud. Este serviço executa compilações no Google Cloud. O Citrix DaaS cria um bucket de armazenamento chamado `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` onde os serviços do Google Cloud capturam informações de log de compilação. Uma opção é definida neste bucket que exclui o conteúdo após um período de 30 dias. Este processo exige que a conta de serviço usada para a conexão tenha as permissões do Google Cloud definidas como `storage.buckets.update`. Se a conta de serviço não tiver essa permissão, o Citrix DaaS ignora os erros e prossegue com o processo de criação do catálogo. Sem essa permissão, o tamanho dos logs de compilação aumenta e requer limpeza manual.

Habilitar acesso privado do Google

Quando uma VM não possui um endereço IP externo atribuído à sua interface de rede, os pacotes são enviados apenas para outros destinos de endereços IP internos. Ao habilitar o acesso privado, a VM se conecta ao conjunto de endereços IP externos usados pela API do Google e serviços associados.

> **Nota:**
>
> Independentemente de o acesso privado do Google estar habilitado, todas as VMs, com e sem endereços IP públicos, devem ser capazes de acessar as APIs Públicas do Google, especialmente se dispositivos de rede de terceiros tiverem sido instalados no ambiente.

Para garantir que uma VM em sua sub-rede possa acessar as APIs do Google sem um endereço IP público para provisionamento MCS:

1. No Google Cloud, acesse a **configuração de rede VPC**.
2. Identifique as sub-redes usadas ou o ambiente Citrix® na guia **Sub-redes no projeto atual**.
3. Clique no nome das sub-redes e ative o **Acesso Privado do Google**.

Para obter mais informações, consulte Configurando o Acesso Privado do Google.

> **Importante:**
>
> Se sua rede estiver configurada para impedir o acesso da VM à internet, certifique-se de que sua organização assuma os riscos associados à habilitação do acesso privado do Google para a sub-rede à qual a VM está conectada.

Onde ir em seguida

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina designada para entregar aplicativos ou um desktop aos seus usuários.
- Para criar e gerenciar conexões, consulte Conexão com ambientes de nuvem do Google.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização HPE Moonshot

O Citrix DaaS™ gerencia suas cargas de trabalho HPE Moonshot por meio de um plug-in HPE Moonshot gerenciado pela Citrix presente no plano de controle do DaaS. Com este plug-in, você pode criar conexões com seu chassi HPE Moonshot, criar catálogos e gerenciar o consumo de energia das máquinas no catálogo.

Etapas principais

1. Configure seus ambientes HPE.
2. Crie uma conexão com o chassi HPE Moonshot.
3. Crie um catálogo de máquinas.

> **Nota:**
>
> Antes de criar um catálogo, certifique-se de ter um ou mais nós de cartucho HPE Moonshot e instale VDAs nesses nós. Você pode considerar o chassi HPE Moonshot como o hipervisor e os nós de cartucho como VMs.

4. Crie um grupo de entrega.
5. Migre o restante dos nós HPE Moonshot não gerenciados para o catálogo ou grupo de entrega gerenciado.

Onde ir em seguida

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que entregará aplicativos ou um desktop aos seus usuários.
- Para criar e gerenciar conexões, consulte Conexão com HPE Moonshot.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização do Microsoft Azure Resource Manager

Ao usar o Microsoft Azure Resource Manager para provisionar máquinas virtuais em sua implantação do Citrix DaaS™, familiarize-se com o seguinte:

- O que é o Microsoft Entra ID?
- Guia de introdução à integração do Microsoft Entra ID com aplicativos
- Objetos de aplicativo e entidade de serviço no Microsoft Entra ID
- Identidades gerenciadas para recursos do Azure

Para configurar seu Microsoft Azure Resource Manager, consulte Configurar local do recurso.

Onde ir em seguida

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina designada para entregar aplicativos ou uma área de trabalho aos seus usuários.
- Para criar e gerenciar conexões, consulte Conexão com o Microsoft Azure.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas
- CTX219211: Configurar uma conta do Microsoft Entra ID
- CTX219243: Conceder acesso do XenApp e XenDesktop à sua assinatura do Azure
- CTX219271: Implantar nuvem híbrida usando VPN site a site

Ambientes de virtualização Microsoft SCVMM

Siga esta orientação se você usa o Hyper-V com o Microsoft System Center Virtual Machine Manager (VMM) para fornecer máquinas virtuais.

Consulte Requisitos do sistema para obter uma lista das versões de VMM compatíveis.

Você pode usar o Machine Creation Services™ ou o Citrix Provisioning (anteriormente Provisioning Services) para provisionar:

- VMs de SO de Desktop ou Servidor de Geração 1
- VMs de Geração 2 do Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10 e Windows 11 (com ou sem inicialização segura)

Instalar e configurar um hipervisor

Instale a função Microsoft Hyper-V e o VMM em seus servidores.

Verifique as seguintes informações da conta:

No Studio, a conta que você especifica ao criar uma conexão deve ser um administrador VMM ou um administrador delegado VMM para as máquinas Hyper-V relevantes. Se esta conta tiver apenas a função de administrador delegado no VMM, os dados de armazenamento não serão listados no Studio durante o processo de criação da conexão.

Sua conta de usuário também deve ser membro do grupo de segurança local de administradores em cada servidor Hyper-V para oferecer suporte ao gerenciamento do ciclo de vida da VM (como criação, atualização e exclusão de VM).

Em grandes implantações onde um único SCVMM gerencia vários clusters em diferentes data centers, você pode limitar o escopo dos grupos de host dos administradores.

Para limitar o escopo dos grupos de host, use a função de administrador delegado no console do Microsoft System Center Virtual Machine Manager (VMM).

1. No **Assistente de Criação de Funções de Usuário**, selecione **Administrador de Malha** (administrador delegado) como uma função de usuário.
2. Em **Membros**, adicione a conta de usuário no Active Directory que você deseja usar como administrador delegado.
3. Em **Escopo**, selecione os grupos de host aos quais você deseja que o administrador delegado tenha acesso.
4. Crie uma nova **Conta Executar como** usando as credenciais de usuário do administrador delegado. Use essas credenciais para criar uma conexão de hipervisor posteriormente. Não use as contas de função de administrador principal.

Instalar o console VMM

Instale um console do System Center Virtual Machine Manager em cada servidor que tenha um Citrix Cloud Connector.

A versão do console deve corresponder à versão do servidor de gerenciamento. Embora um console anterior possa se conectar ao servidor de gerenciamento, o provisionamento de VDAs falha se as versões forem diferentes.

Onde ir em seguida

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina designada para entregar aplicativos ou um desktop aos seus usuários.
- Para criar e gerenciar conexões, consulte Conexão com o Microsoft System Center Virtual Machine Manager.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização Nutanix

Conecte o Citrix DaaS™ a clusters Nutanix AHV por meio do Nutanix Prism Central usando a conexão de host Nutanix AHV Prism Central. Esta conexão de host:

- Suporta catálogos de máquinas com VDAs gerenciados por energia e provisionados por MCS.
- Permite o compartilhamento de imagem mestre MCS entre clusters AHV usando versões de modelo.
- Simplifica a confiança do certificado na conexão do host.
- Elimina a necessidade de instalação do plug-in Nutanix nos Cloud Connectors.

Consulte Nutanix Prism Central no AHV.

Você também pode usar o Nutanix Prism Element no AHV usando o Nutanix Acropolis como conexão de host para fornecer VMs em sua implantação do Citrix DaaS. No entanto, este processo de configuração requer a instalação e o registro do plug-in Nutanix em seu ambiente Citrix DaaS. Consulte Nutanix Prism Element no AHV.

Para obter mais informações sobre o guia de instalação do plug-in Nutanix Acropolis MCS, consulte o Portal de Suporte Nutanix.

Nutanix Prism Central no AHV

A Citrix desenvolveu e mantém um plug-in que integra o Citrix ao Nutanix Prism Central no AHV. Este plug-in é integrado aos Citrix Delivery Controllers, eliminando a necessidade de instalações de plug-ins separadas.

O plug-in Nutanix AHV Prism Central é pré-instalado nos Delivery Controllers gerenciados pela Citrix no Citrix DaaS, eliminando a necessidade de instalação separada nos Cloud Connectors. Para obter informações sobre componentes e serviços gerenciados pela Citrix, consulte Componentes e serviços gerenciados pela Citrix.

Pré-requisitos

Você precisa do seguinte para o Nutanix AHV Prism Central:

- Versão do Prism Central pc.2025.2 ou posterior. Consulte Hipervisores suportados para Citrix Virtual Apps and Desktops (MCS) e Citrix Provisioning (PVS) para obter as versões detalhadas do Prism Central suportadas.
- A versão AOS 7.3 ou posterior para os clusters Nutanix AHV.
- Os clusters Nutanix AHV devem se registrar no Prism Central.
- A conta de administrador Citrix deve ter permissões suficientes para criar conexões de host, catálogos de máquinas e grupos de entrega. Para obter mais informações, consulte Configurar Administração Delegada.
- O Citrix Cloud™ se comunica com o Nutanix Prism Central através do Cloud Connector. Portanto, a instância do Nutanix Prism Central deve estar acessível a partir do Cloud Connector.

Limitações no recurso

Devido a limitações do Nutanix Prism e da API, ações de energia como Reinicialização do Convidado ou Desligamento do Convidado podem falhar para uma VM Windows. Para resolver esse problema, recomendamos seguir as instruções da Nutanix no documento Ações de energia iniciadas do Prism ou da API podem falhar para VMs Windows para aplicar configurações nos VDAs.

Etapas principais

1. Configure seus ambientes de virtualização Nutanix. Para obter informações, consulte Adicionar um tipo de recurso ou Ativar um domínio não utilizado.
2. Criar uma conexão com o Nutanix AHV Prism Central
3. Criar um catálogo de máquinas usando a versão do modelo de máquina Nutanix.

Nutanix Prism Element no AHV

O Nutanix Prism Element no AHV requer a instalação do plug-in Nutanix em todos os Cloud Connectors onde o Citrix DaaS deve criar uma conexão de host com o local de recurso que possui um hipervisor Nutanix.

Etapas principais

1. Instale e registre o plug-in Nutanix.
2. Configure seus ambientes de virtualização Nutanix. Para obter informações, consulte Adicionar um tipo de recurso ou Ativar um domínio não utilizado.
3. Criar uma conexão.
4. Criar um catálogo de máquinas.

Instalar e registrar o plug-in Nutanix

Conclua o procedimento para instalar e registrar o plug-in Nutanix em todos os seus Cloud Connectors. Para obter informações sobre a instalação do plug-in Nutanix, consulte o site de documentação da Nutanix.

Onde ir em seguida

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina designada para entregar aplicativos ou um desktop aos seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com Nutanix.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Soluções de nuvem e parceiros Nutanix

Nutanix AHV Prism Central

O Citrix DaaS™ oferece suporte a Nutanix Cloud Clusters (NC2) nos seguintes hipervisores de nuvem para o plug-in Nutanix AHV Prism Central gerenciado pela Citrix.

- Amazon Web Services (AWS)
- Microsoft Azure

Nutanix Cloud Clusters

O Citrix DaaS oferece suporte a Nutanix Cloud Clusters no AWS e Azure. Os clusters Nutanix simplificam a forma como os aplicativos são executados em nuvens privadas ou em várias nuvens públicas.

Para obter mais informações sobre como configurar o NC2, consulte:

- Guia de Implantação e Usuário do Nutanix Cloud Clusters no AWS
- Guia de Implantação e Usuário do Nutanix Cloud Clusters no Azure.

Requisitos

Você precisa das seguintes contas para usar o NC2:

- Uma conta Nutanix
- Para AWS: Uma conta AWS com as seguintes permissões.
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess
- Para Azure:
  - Uma licença válida de “NC2 on Azure”
  - Uma conta Azure que inclua uma das seguintes funções:
    - Global Administrator
    - Cloud Application Administrator
    - Application Administrator
    - todas as permissões

Permissões para NC2 no Azure

```
Microsoft.Compute/register/action

Microsoft.Compute/availabilitySets/write

Microsoft.Compute/availabilitySets/delete

Microsoft.Compute/disks/read

Microsoft.Compute/disks/write

Microsoft.Compute/disks/delete

Microsoft.Compute/locations/usages/read
```

```
Microsoft.Compute/availabilitySets/read

Microsoft.Compute/virtualMachines/*

Microsoft.Compute/snapshots/*

Microsoft.Compute/images/*

Microsoft.Network/register/action

Microsoft.Network/natGateways/*

Microsoft.Network/networkInterfaces/*

Microsoft.Network/networkSecurityGroups/*

Microsoft.Network/publicIPAddresses/*

Microsoft.Network/virtualNetworks/*

Microsoft.Network/locations/usages/read

Microsoft.Storage/register/action

Microsoft.Storage/checknameavailability/read Microsoft.Storage/locations/
checknameavailability/read Microsoft.Storage/locations/usages/read

Microsoft.Storage/storageAccounts/write

Microsoft.Storage/storageAccounts/read

Microsoft.Storage/storageAccounts/delete Microsoft.Storage/
storageAccounts/blobServices/containers/clearLegalHold/action
Microsoft.Storage/storageAccounts/blobServices/containers/delete
Microsoft.Storage/storageAccounts/blobServices/containers/lease/action

Microsoft.Storage/storageAccounts/blobServices/containers/ read
Microsoft.Storage/storageAccounts/blobServices/containers/ write
Microsoft.Storage/storageAccounts/blobServices/read Microsoft.Storage/
storageAccounts/blobServices/write Microsoft.Storage/storageAccounts/
listAccountSas/action Microsoft.Storage/storageAccounts/listkeys/action
Microsoft.Storage/storageAccounts/listServiceSas/action Microsoft.Storage/
storageAccounts/regeneratekey/action Microsoft.Storage/storageAccounts/
```

```
revokeUserDelegationKeys/action Microsoft.ResourceHealth/
AvailabilityStatuses/read Microsoft.ResourceHealth/events/read

Microsoft.ResourceHealth/AvailabilityStatuses/current/read

Microsoft.ManagedIdentity/userAssignedIdentities/* Microsoft.Resources/
subscriptions/locations/read Microsoft.Resources/subscriptions/
resourceGroups/read Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourcegroups/deployments/read

Microsoft.Resources/subscriptions/resourcegroups/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/resources/read
Microsoft.Resources/subscriptions/tagNames/read Microsoft.Resources/
subscriptions/tagNames/write Microsoft.Resources/subscriptions/tagNames/
delete Microsoft.Resources/subscriptions/tagNames/tagValues/write
Microsoft.Resources/subscriptions/tagNames/tagValues/read
Microsoft.Resources/subscriptions/tagNames/tagValues/delete
Microsoft.Resources/tags/read

Microsoft.Resources/tags/write

Microsoft.Resources/tags/delete

Microsoft.Resources/providers/read

Microsoft.Compute/sshPublicKeys/read

Microsoft.Compute/sshPublicKeys/write

Microsoft.Compute/sshPublicKeys/delete Microsoft.Compute/sshPublicKeys/
generateKeyPair/action Microsoft.Nutanix/Interfaces/read

Microsoft.Nutanix/Interfaces/write

Microsoft.Nutanix/Interfaces/delete

Microsoft.Nutanix/Nodes/read

Microsoft.Nutanix/Nodes/write

Microsoft.Nutanix/Nodes/delete

Microsoft.Nutanix/register/action
```

```
Microsoft.Network/virtualHubs/*

Microsoft.Network/routeTables/read

Microsoft.Network/routeTables/write

Microsoft.Network/routeTables/delete

Microsoft.Network/routeTables/join/action

Microsoft.Network/routeTables/routes/read Microsoft.Network/routeTables/
routes/write Microsoft.Network/routeTables/routes/delete
Microsoft.CostManagement/query/read

Microsoft.CostManagement/views/read Microsoft.CostManagement/
externalSubscriptions/query/read Microsoft.CostManagement/
externalSubscriptions/dimensions/read Microsoft.CostManagement/
externalSubscriptions/read Microsoft.CostManagement/
externalBillingAccounts/forecast/read

Microsoft.CostManagement/externalBillingAccounts/read

Microsoft.CostManagement/externalBillingAccounts/query/read
Microsoft.CostManagement/externalBillingAccounts/ externalSubscriptions/
read Microsoft.CostManagement/externalSubscriptions/forecast/read
Microsoft.CostManagement/operations/read Microsoft.CostManagement/
forecast/read

Microsoft.Network/virtualWans/write

Microsoft.Network/virtualWans/read

Microsoft.Network/virtualWans/delete Microsoft.Network/virtualWans/
virtualHubs/read Microsoft.Network/virtualWans/join/action
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ read
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ write
Microsoft.Network/virtualHubs/hubVirtualNetworkConnections/ delete
Microsoft.Network/privateEndpoints/pushPropertiesToResource/ action
Microsoft.Network/privateEndpoints/read

Microsoft.Network/privateEndpoints/write Microsoft.Network/
privateEndpoints/delete Microsoft.Network/privateDnsZones/read
Microsoft.Network/privateDnsZones/delete Microsoft.Network/
```

```
privateDnsZones/join/action Microsoft.Network/privateDnsZones/write
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/ write

Microsoft.Network/privateEndpoints/privateDnsZoneGroups/read
Microsoft.Network/privateEndpoints/privateDnsZoneGroups/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
deleteBlobVersion/action

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/
read Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/
read

Microsoft.Storage/storageAccounts/blobServices/containers/blobs/tags/write
Microsoft.Storage/storageAccounts/blobServices/containers/ blobs/write
Microsoft.Storage/storageAccounts/blobServices/containers/blobs/filter/
action Microsoft.Storage/storageAccounts/blobServices/containers/blobs/
modifyPermissions/action
```

Criar um Cluster Nutanix

1. Faça login na sua conta Nutanix.
2. navegar até a opção de cluster Nutanix e clique em **Launch**. O **Nutanix Console** é aberto. Para mais informações:
   - Introdução ao Cluster Nutanix no AWS
   - Nutanix Cloud Clusters on Microsoft Azure
3. Selecione a opção para criar uma nova VPC.

Assim que o cluster for criado, recupere o endereço do Nutanix Prism.

SOLUÇÃO DE PROBLEMAS

O processo de criação do cluster pode falhar com os seguintes erros:

- **Falha ao criar o cluster dentro do tempo especificado. Excluindo cluster**
- **Host Nutanix Cluster - Nó XXXXXXXXXXX: Instância i-xxxxxxxxxxxxx: erro ao desabilitar a verificação de origem/destino da interface de rede**.

- **Host Nutanix Cluster - Nó XXXXXXXXXXX: Não foi possível obter informações da interface de rede da instância i-xxxxxxxxxxxxx**

Se o cluster falhar ao ser criado, tente recriá-lo em uma região diferente. Certifique-se de excluir o Nutanix CloudFormation Stack (CFS) antes de tentar novamente.

> **Nota:**

> Além de outros recursos, o Nutanix CFS cria:

> - Uma VPC chamada Nutanix Cluster xxxxxxxxxxxx 10.0.0.0/16
> - Duas sub-redes 10.0.128.0/24 e 10.0.129.0/24
> - Um gateway de Internet
> - Um gateway NAT

Recuperar o endereço do servidor Prism

1. Registre o cluster NC2 com o servidor Prism Central. Consulte Registrando um Cluster com o Prism Central.
2. Use o nome do host ou o endereço IP do servidor Prism Central como o endereço.

NC2 para Nutanix Prism Element

O Citrix DaaS oferece suporte a Nutanix Cloud Clusters (NC2) no seguinte hipervisor de nuvem para o plug-in Nutanix Prism Element.

- Amazon Web Services (AWS)

Nutanix Cloud Clusters no AWS

Para obter mais informações sobre Nutanix Cloud Clusters no AWS, consulte Guia do Usuário e Implantação de Nutanix Cloud Clusters no AWS.

> **Dica:**

> Este suporte oferece a mesma funcionalidade de um cluster Nutanix local. Apenas um único cluster é suportado, o *Prism Element*. Para obter mais informações, consulte aqui.

> Você precisa das seguintes contas para usar o NC2 no AWS:

- Uma conta Nutanix
- Uma conta AWS com as seguintes permissões:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Para criar um Cluster Nutanix e solucionar problemas caso a criação do cluster falhe, consulte Criar um Cluster Nutanix e Solução de problemas.

Depois que o cluster for criado, recupere o endereço do **Nutanix Prism**:

Recuperar o endereço do servidor Prism

1. Vá para o **Console Nutanix**.
2. No canto superior direito do console, passe o mouse sobre o link **Launch Prism Element** e copie o URL.

Onde ir em seguida

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina designada para entregar aplicativos ou um desktop aos seus usuários.
- Para criar e gerenciar conexões, consulte Conexão com soluções de nuvem e parceiros Nutanix.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização Red Hat OpenShift

A Citrix® gerencia suas cargas de trabalho do Red Hat OpenShift por meio de um plug-in OpenShift gerenciado pela Citrix. Com este plug-in, você pode criar conexões de hospedagem e unidades de hospedagem para seu cluster OpenShift, criar catálogos e gerenciar o consumo de energia das máquinas no catálogo.

As seguintes configurações são suportadas:

- Opções de rede:
  - Linux Bridge e OVS Bridge: Disponíveis para rede de cluster.
- Opções de armazenamento:
  - Armazenamento local: Suportado para armazenamento persistente no nó.
  - Armazenamento NetApp: Suportado para integração de armazenamento externo de nível empresarial.

Etapas principais

- Configure seu ambiente Red Hat OpenShift.
- Crie uma conexão e um recurso para o cluster OpenShift.
- Crie um catálogo de máquinas.
- Crie um grupo de entrega.

Configure seu ambiente Red Hat OpenShift

1. *Crie um cluster OpenShift e obtenha o endereço da API do cluster*: No console do OpenShift, após configurar um cluster, navegar para **Home > Overview > Details** e obtenha o endereço da API do cluster.
2. *Crie uma conta de serviço e obtenha o token da conta de serviço usando a interface de linha de comando (CLI) do OpenShift (comando oc)*: O token da conta de serviço é a credencial de autenticação associada à conta de serviço. A conta de serviço é usada para autenticar o plug-in do OpenShift com o OpenShift. Cada conta de serviço está associada a um namespace.
3. *Configure as permissões para a conta de serviço*: Uma conta de serviço pode ter várias funções, e cada função consiste em permissões que definem quais ações o Plug-in do OpenShift pode executar em quais recursos. As funções são vinculadas por meio de **Associações de Função (Role Bindings)**, e existem dois tipos de **Associações de Função (Role Bindings)**:
   a. **Associação de Função (Role Binding) em todo o Cluster**: usada para receber eventos do OpenShift. Associação de Função (Role Binding) vinculada ao Namespace: usada para gerenciar VMs em um namespace específico.
   b. **Associação de Função (Role Binding) vinculada ao Namespace**: usada para gerenciar VMs em um namespace específico.
4. *Crie um namespace (Projeto)*: Namespace no OpenShift é um ambiente isolado que agrupa recursos como VMs ou redes, permitindo melhor organização e controle de acesso.

Namespace é o termo do Kubernetes, enquanto **Projeto** é o termo do OpenShift. Da perspectiva do Plug-in do OpenShift, eles são os mesmos. Um namespace é necessário para implantar as VMs. Use o console do OpenShift ou a CLI da Plataforma de Contêineres do OpenShift para criar o namespace.

5. *Crie uma definição de anexo de rede no namespace de destino*: As definições de anexo de rede especificam a configuração de rede para VMs em execução no OpenShift. Em **Rede (Networking) > Definições de Anexo de Rede (NetworkAttachmentDefinitions)**, você pode ver as Definições de Anexo de Rede para cada Namespace.
6. *Configure as classes de armazenamento*: As classes de armazenamento definem como o armazenamento de VM é alocado. Em **Armazenamento (Storage) > Classe de Armazenamento (StorageClass)**, você pode configurar e ver a lista de provedores de armazenamento.

Criar uma conta de serviço

1. Baixe e descompacte a Ferramenta de Linha de Comando oc.
2. Acesse o Console do OpenShift usando seu ID de login.
3. Clique no seu perfil de usuário e clique em **Copiar comando de login**.
4. Clique em **Exibir Token** e copie o token.
5. Execute o comando de login usando a Linha de Comando oc. Exemplo:

```
.\oc.exe login --token=<token> --server=<server address>
```

6. Crie uma conta de serviço.
   - Se você deseja criar a conta de serviço no namespace padrão, execute:

```
.\oc.exe create sa <service account name>
```

   - Se você quiser criar a conta de serviço em seu próprio namespace, execute:

```
.\oc.exe create sa <service account name> -n mynamespace
```

7. Crie um arquivo `YAML` para o segredo. Exemplo:
   - Se você criar a conta de serviço no namespace padrão:

```
apiVersion: v1

kind: Secret

metadata:

name: service account name

annotations:

kubernetes.io/service-account.name: service account name

type: kubernetes.io/service-account-token
```

- Se você criar a conta de serviço em seu próprio namespace:

```
apiVersion: v1

kind: Secret

metadata:

name: service account name

namespace: mynamespace

annotations:

kubernetes.io/service-account.name: service account name

 type: kubernetes.io/service-account-token
```

8. Aplique o YAML.

```
.\oc.exe apply -f <yamlFile.yaml>
```

Nota:

O `oc` descreve o segredo para obter o token. O token é usado como uma senha.

Criar funções e vinculações de função para a conta de serviço

Com a vinculação de função em todo o cluster, a conta de serviço tem permissões para ler todos os eventos de VM em todo o cluster, permitindo que o plug-in do OpenShift mantenha um único observador de eventos para todos os eventos relacionados à VM. Com a vinculação de função de namespace, a conta de serviço tem permissões para gerenciar VMs no namespace de destino. Você pode usar um script para criar funções e vinculá-las a uma conta de serviço. Consulte `<https://github.com/citrix/citrix-mcs-sdk-samples/tree/main/OpenShift/Hosting%20Connection/Role/>`.

Onde ir em seguida

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina que entregará aplicativos ou uma área de trabalho aos seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com o Red Hat OpenShift

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização VMware

Siga esta orientação se você usa VMware para fornecer máquinas virtuais.

Instale o vCenter Server e as ferramentas de gerenciamento apropriadas. (Nenhum suporte é fornecido para a operação do vSphere vCenter Linked Mode.)

> **Nota:**
>
> Nenhum suporte é fornecido para a operação do vSphere vCenter Linked Mode.
>
> Se você planeja usar o Machine Creation Services™ (MCS), não desative o recurso Datastore Browser no vCenter Server. Se você desativar esse recurso, o MCS não funcionará corretamente.

Para configurar seus ambientes de virtualização VMware, consulte Adicionar um tipo de recurso ou ativar um domínio não utilizado no Citrix Cloud.

Onde ir em seguida

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina designada para entregar aplicativos ou um desktop aos seus usuários.
- Para criar e gerenciar conexões, consulte Conexão com VMware.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Soluções de nuvem e parceiros VMware

O Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™) oferece suporte às seguintes soluções de nuvem e parceiros VMware:

- Azure VMware Solution (AVS)
- Google Cloud VMware Engine
- VMware Cloud on Amazon Web Services (AWS)

Use o Citrix DaaS™ para migrar cargas de trabalho Citrix locais baseadas em VMware para as respectivas soluções de parceiros VMware.

Integração do Azure VMware Solution (AVS)

O Citrix DaaS oferece suporte ao AVS. O AVS fornece infraestrutura de nuvem contendo clusters vSphere criados pela infraestrutura do Azure. Aproveite o DaaS para usar o AVS para provisionar sua carga de trabalho VDA da mesma forma que você usaria o vSphere em ambientes locais.

Configurar o cluster AVS

Para permitir que o Citrix DaaS use o AVS, execute as seguintes etapas no Azure:

- Solicitar uma cota de host
- Registrar o provedor de recursos `Microsoft.AVS`
- Verificar a lista de verificação de planejamento de rede
- Lista de Verificação de Rede
- Criar uma nuvem privada AVS
- Acessar a nuvem privada AVS

- Configurar a rede para sua nuvem privada VMware no Azure
- Configurar DHCP para AVS
- Adicionar um segmento de rede no AVS
- Verificar o ambiente AVS

SOLICITAR COTA DE HOST PARA CLIENTES DO CONTRATO ENTERPRISE DO AZURE

Na página **Ajuda + Suporte** do portal do Azure, selecione **Nova solicitação de suporte** e inclua as seguintes informações:

- Tipo de problema: Técnico
- Assinatura: Selecione sua assinatura
- Serviço:**Todos os serviços > Azure VMware Solution**
- Recurso: Pergunta geral
- Resumo: Necessidade de capacidade
- Tipo de problema: Problemas de Gerenciamento de Capacidade
- Subtipo de problema: Solicitação do Cliente para Cota/Capacidade de Host Adicional

Na **Descrição** do tíquete de suporte, inclua as seguintes informações na guia **Detalhes**:

- POC ou Produção
- Nome da Região
- Número de hosts
- Quaisquer outros detalhes

> **Nota:**

> O AVS requer um mínimo de três hosts e recomenda que você use redundância de hosts N+1.

> Após especificar os detalhes para o tíquete de suporte, selecione **Revisar + Criar** para enviar a solicitação ao Azure.

REGISTRAR O PROVEDOR DE RECURSOS MICROSOFT.AVS

Após solicitar a cota de host, registre o provedor de recursos:

1. Faça login no portal do Azure.

2. No menu do portal do Azure, selecione **Todos os serviços**.
3. No menu **Todos os serviços**, insira a assinatura e selecione **Assinaturas**.
4. Selecione a assinatura na lista de assinaturas.
5. Selecione **Provedores de recursos** e insira **Microsoft.AVS** na barra de pesquisa.
6. Se o provedor de recursos não estiver registrado, selecione **Registrar**.

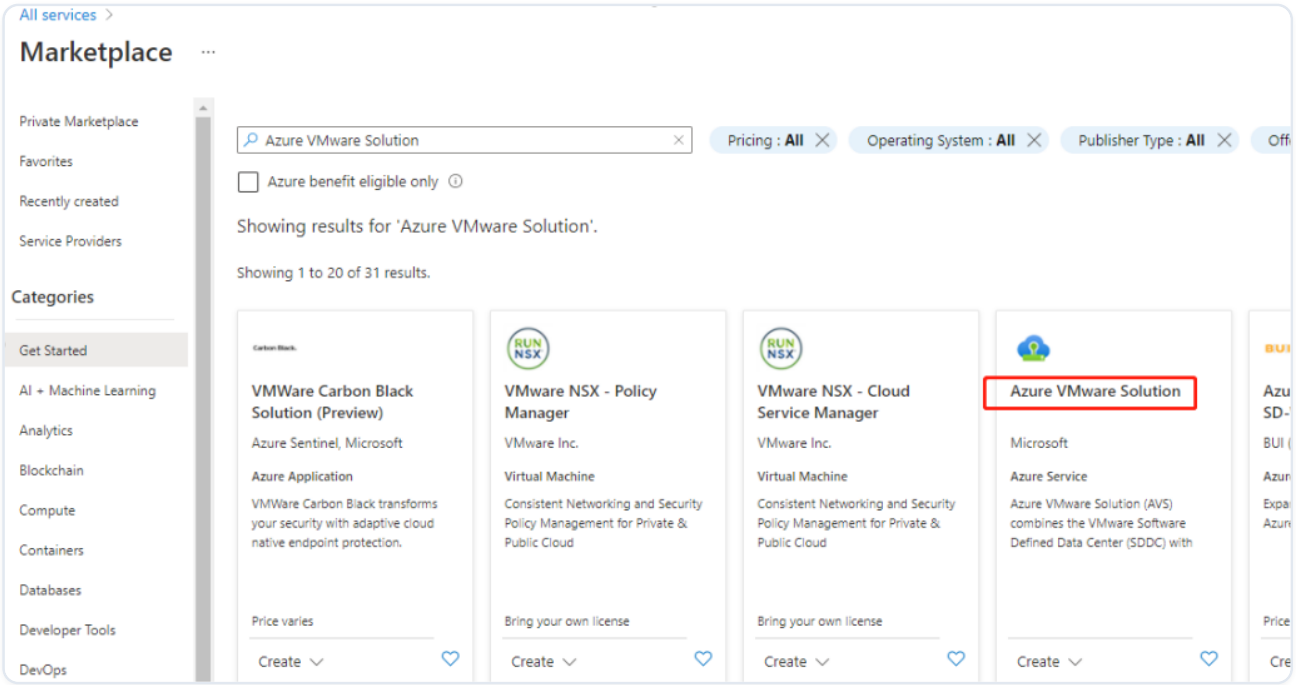
CONSIDERAÇÕES DE REDE

O AVS oferece serviços de rede que exigem intervalos de endereços de rede específicos e portas de firewall. Consulte Lista de verificação de planejamento de rede para a Solução VMware do Azure para obter mais informações.

CRIAR UMA NUVEM PRIVADA AVS

Depois de considerar os requisitos de rede para seu ambiente, crie uma nuvem privada ASV:

1. Faça login no portal do Azure.
2. Selecione **Criar um novo recurso**.
3. Na caixa de texto **Pesquisar no Marketplace**, digite *Azure VMware Solution* e selecione **Azure VMware Solution** na lista.



Na janela **Azure VMware Solution**:

1. Selecione **Criar**.
2. Vá para a guia **Básico**.
3. Insira os valores para os campos, usando as informações na tabela abaixo:

CAMPO	VALOR
Assinatura	Selecione a assinatura que você planeja usar para a implantação. Todos os recursos em uma assinatura do Azure são cobrados juntos.
Grupo de recursos	Selecione o grupo de recursos para sua nuvem privada. Um grupo de recursos do Azure é um contêiner lógico no qual os recursos do Azure são implantados e gerenciados. Alternativamente, você pode criar um novo grupo de recursos para sua nuvem privada.
Localização	Selecione um local, como leste dos EUA. Esta é a região que você definiu durante a fase de planejamento.
Nome do recurso	Forneça o nome da sua nuvem privada do Azure VMware Solution.
Tamanho do host	Selecione o tamanho de acordo com sua necessidade.
Número de hosts	Mostra o número de hosts alocados para o cluster da nuvem privada. O valor padrão é 3, que pode ser aumentado ou diminuído após a implantação.
Bloco de endereços para nuvem privada	Forneça um bloco de endereços IP para a nuvem privada. O CIDR representa a rede de gerenciamento da nuvem privada e será usado para os serviços de gerenciamento de cluster, como vCenter Server e NSX-T Manager. Use o espaço de endereço /22, por exemplo, 10.175.0.0/22. O endereço deve ser exclusivo e não se sobrepor a outras Redes Virtuais do Azure e a redes locais.

Na tela **Criar uma nuvem privada**:

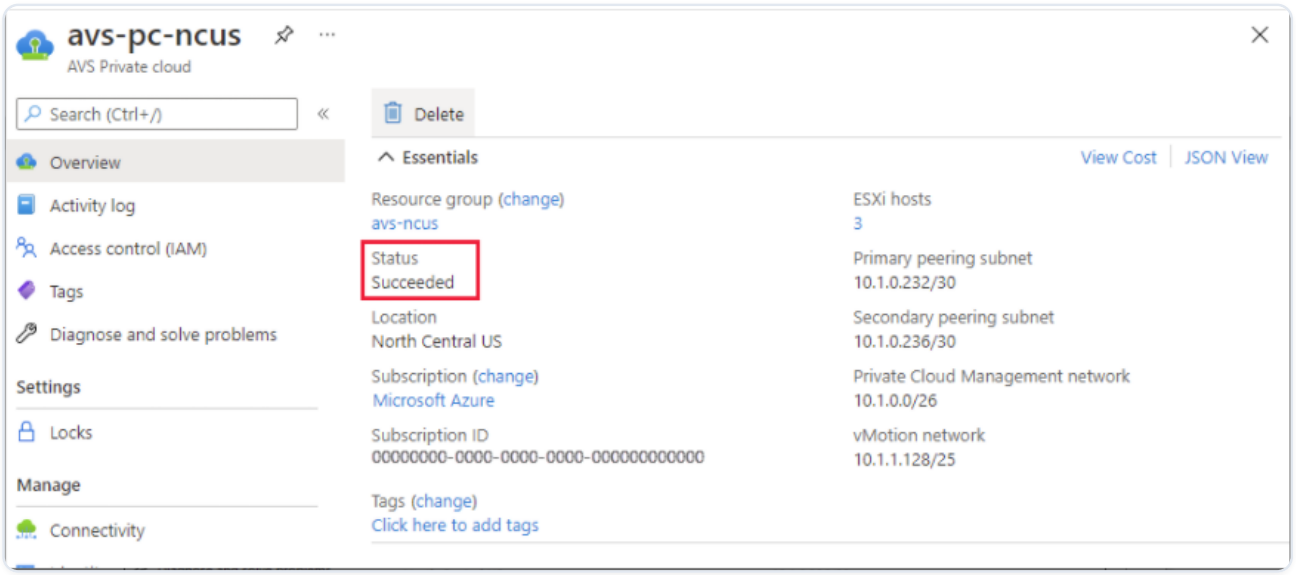
1. No campo **Localização**, selecione a região que possui o AVS. A região do grupo de recursos é a mesma da região do AVS.

2. No campo **Tamanho do host**, selecione um tamanho conforme sua necessidade.
3. Especifique um endereço IP no campo **Bloco de endereço para nuvem privada**. Por exemplo, 10.15.0.0/22.
4. Selecione **Revisar + Criar**.
5. Após revisar as informações, clique em **Criar**.

> **Dica:**

> A criação de uma nuvem privada pode levar de 3 a 4 horas. Adicionar um único host ao cluster pode levar de 30 a 45 minutos.

> Verifique se a implantação foi bem-sucedida. navegar até o grupo de recursos que você criou e selecione sua nuvem privada. Assim que o **Status** for **Bem-sucedido**, a implantação estará concluída.



ACESSAR A NUVEM PRIVADA AVS

Depois de criar uma nuvem privada, crie uma VM Windows e conecte-se ao vCenter local da sua nuvem privada.

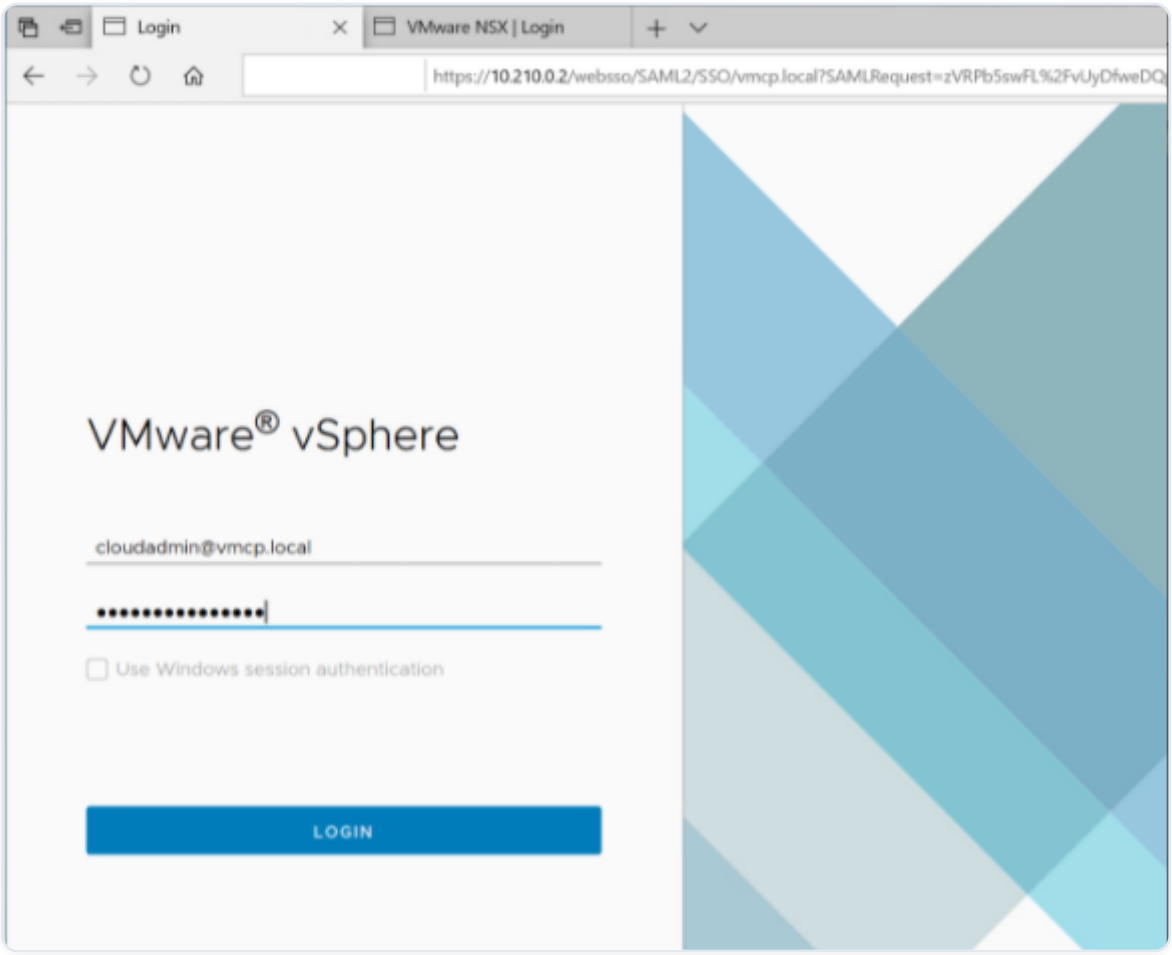
Criar uma nova máquina virtual Windows

1. No grupo de recursos, selecione **+ Adicionar**, depois pesquise e selecione **Microsoft Windows 10/11 ou Windows Server 2016/2019**.
2. Insira as informações necessárias e selecione **Revisar + Criar**.

3. Assim que a validação for aprovada, selecione **Criar** para iniciar o processo de criação da máquina virtual.

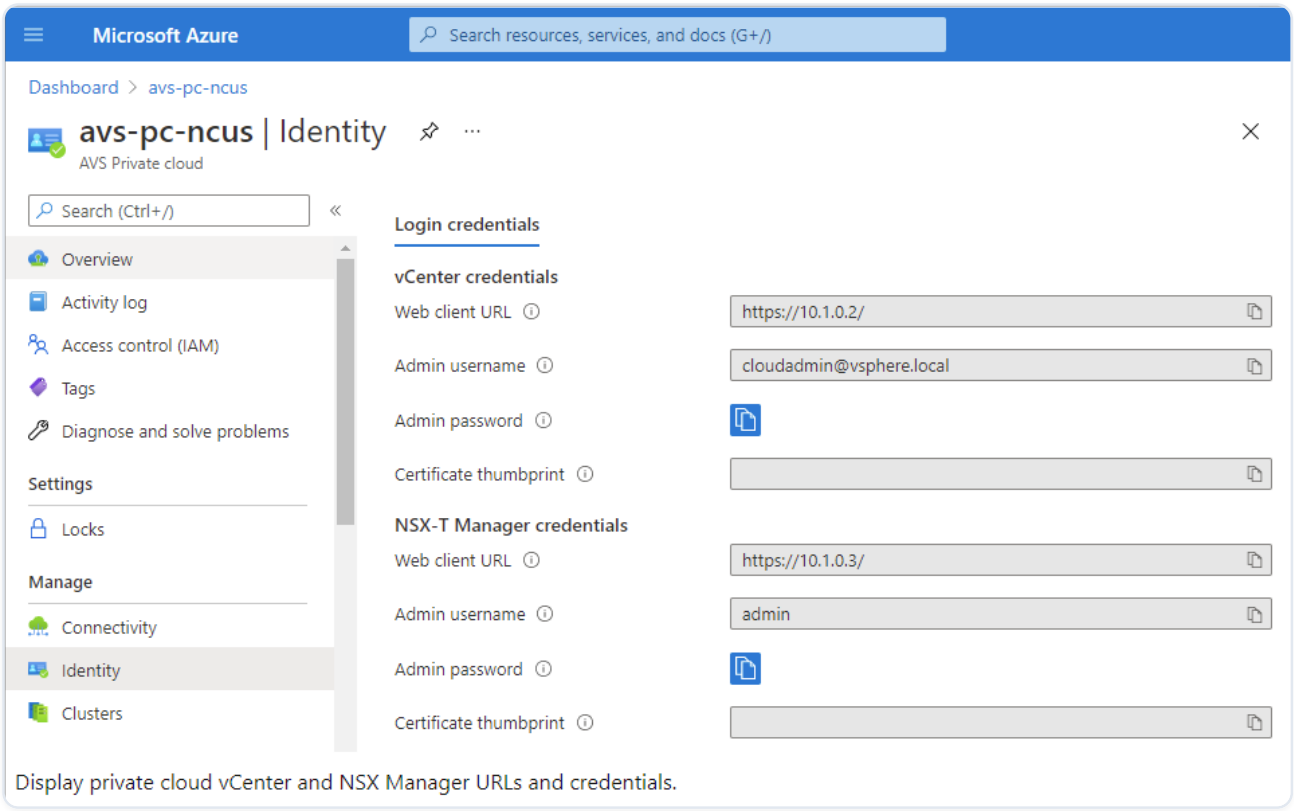
Conectar-se ao vCenter local da sua nuvem privada

1. Faça login no **vSphere Client com VMware vCenter SSO** como administrador de nuvem.



2. No portal do Azure, selecione sua nuvem privada e, em seguida, **Gerenciar > Identidade**.

As URLs e as credenciais de usuário para o vCenter da nuvem privada e o NSX-T Manager aparecem:



Após confirmar as URLs e as credenciais de usuário:

1. navegar para a VM que você criou na etapa anterior e conecte-se à máquina virtual.
2. Na VM do Windows, abra um navegador e navegar para as URLs do vCenter e do NSX-T Manager em duas guias do navegador. Na guia do vCenter, insira as credenciais de usuário mailto:cloudadmin@vmcp.local da etapa anterior.

CONFIGURAR REDE PARA SUA NUVEM PRIVADA VMWARE NO AZURE

Após acessar uma nuvem privada ASV, configure a rede criando uma rede virtual e um gateway.
Criar uma rede virtual

1. Faça login no portal do Azure.
2. navegar para o grupo de recursos criado anteriormente.
3. Selecione **+ Adicionar** para definir um novo recurso.
4. Na caixa de texto **Pesquisar no Marketplace**, digite *rede virtual*. Encontre o recurso de rede virtual e selecione-o.
5. Na página **Rede Virtual**, selecione **Criar** para configurar a rede virtual para sua nuvem privada.
6. Na página **Criar Rede Virtual**, insira os detalhes da sua rede virtual.
7. Na guia **Básico**, insira um nome para a rede virtual, selecione a região apropriada e clique em **Avançar: Endereços IP.**

8. Na guia **Endereços IP**, em espaço de endereço IPv4, insira o endereço criado anteriormente.

> **Importante:**
>
> Use um endereço que não se sobreponha ao espaço de endereço que você usou ao criar sua nuvem privada.

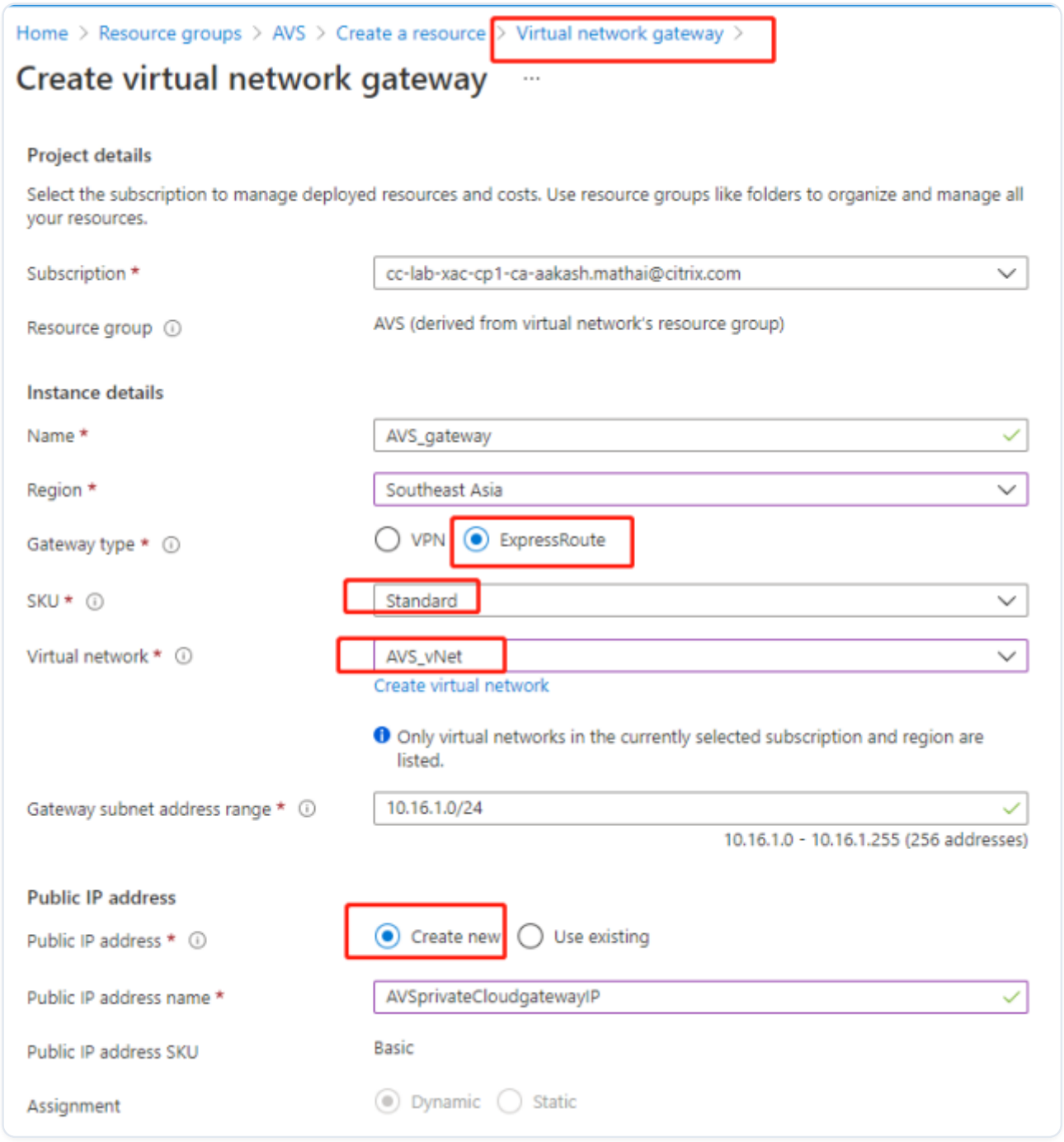
> Após inserir o espaço de endereço:

1. Selecione **+ Adicionar sub-rede**.
2. Na página **Adicionar sub-rede**, dê um nome à sub-rede e um intervalo de endereços apropriado.
3. Clique em **Adicionar.**
4. Selecione **Revisar + criar**.
5. Verifique as informações e clique em **Criar**. Assim que a implantação for concluída, a rede virtual aparecerá no grupo de recursos.

Criar um gateway de rede virtual

Após criar uma rede virtual, crie um gateway de rede virtual.

1. No seu grupo de recursos, selecione **+ Adicionar** para adicionar um novo recurso.
2. Na caixa de texto **Pesquisar no Marketplace**, digite *gateway de rede virtual*. Encontre o recurso de rede virtual e selecione-o.
3. Na página **Gateway de Rede Virtual**, clique em **Criar**.
4. Na guia **Básico** da página **Criar gateway de rede virtual**, forneça valores para os campos.
5. Clique em **Revisar + criar**.



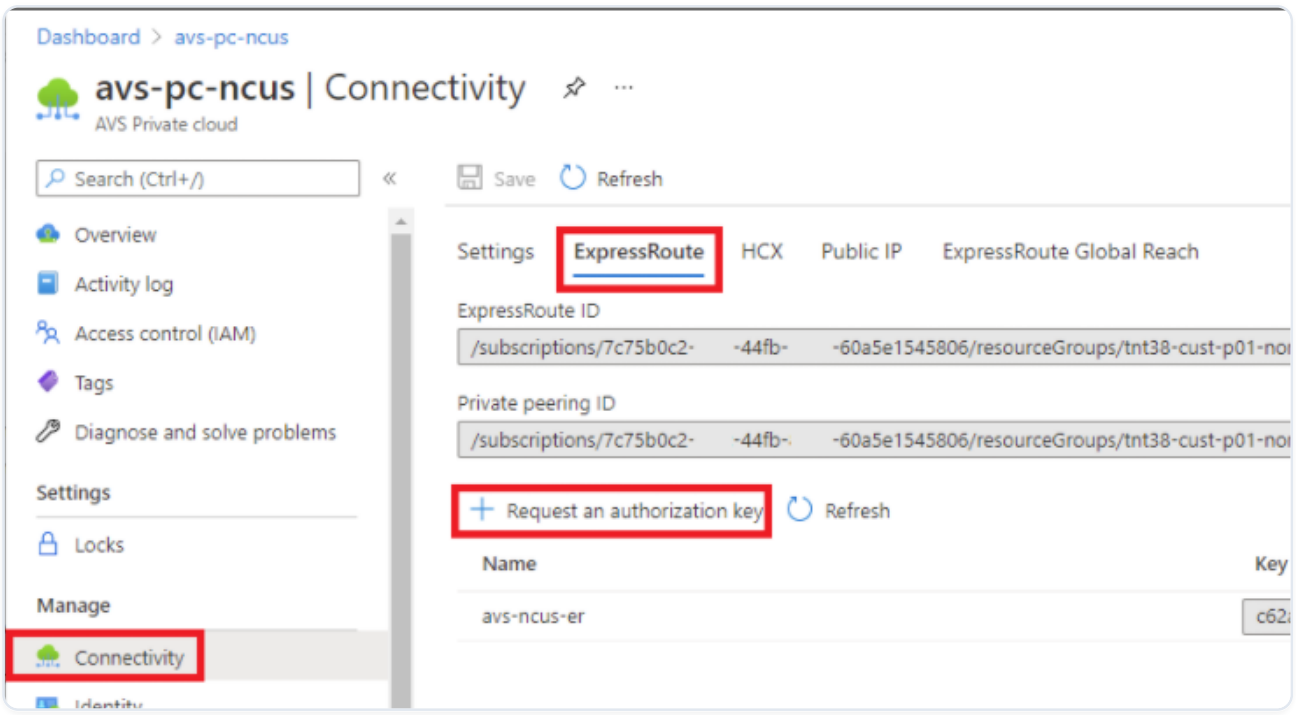
Após revisar a configuração do gateway de rede virtual, clique em **Criar** para implantar seu gateway de rede virtual. Assim que a implantação for concluída, conecte sua conexão **ExpressRoute** ao gateway de rede virtual que contém sua nuvem privada Azure AVS.

CONECTAR O EXPRESSROUTE AO GATEWAY DE REDE VIRTUAL

Após implantar um gateway de rede virtual, adicione uma conexão entre ele e sua nuvem privada Azure AVS:

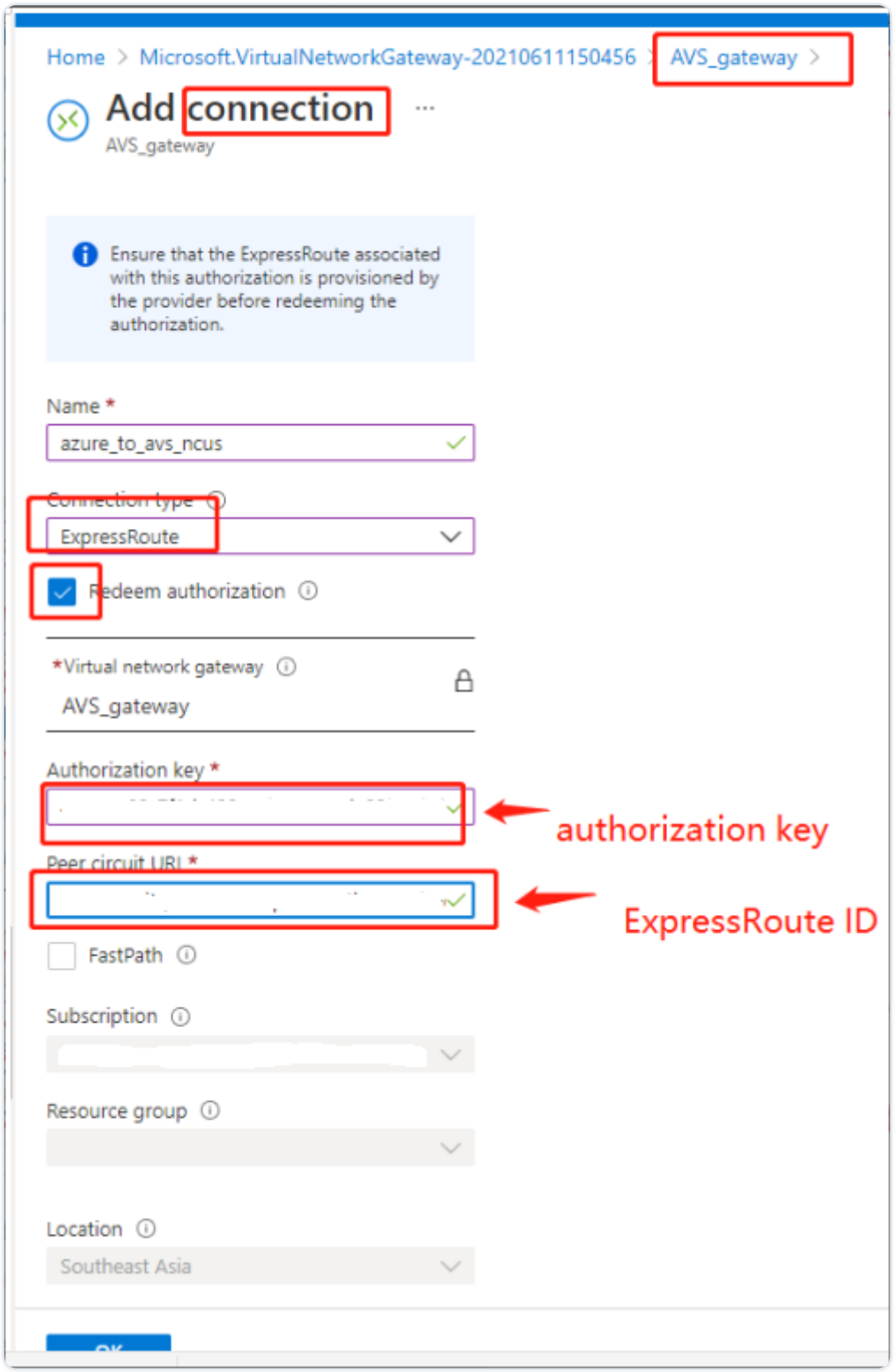
1. Solicite uma chave de autorização do ExpressRoute.

2. No portal do Azure, navegar até a **nuvem privada da Solução VMware do Azure**. Selecione **Gerenciar > Conectividade > ExpressRoute** e, em seguida, selecione **+ Solicitar uma chave de autorização.**

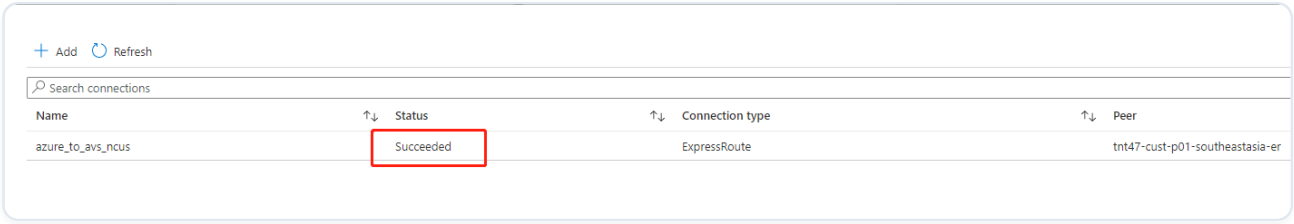


Após solicitar uma chave de autorização:

1. Insira um nome para a chave e clique em **Criar**. Pode levar cerca de 30 segundos para criar a chave. Uma vez criada, a nova chave aparece na lista de chaves de autorização para a nuvem privada.
2. Copie a **chave de autorização** e o **ID do ExpressRoute**. Você precisará deles para concluir o processo de emparelhamento. A chave de autorização desaparece após algum tempo, então copie-a quando ela aparecer.
3. navegar até o **gateway de rede virtual** que você planeja usar e selecione **Conexões > + Adicionar**.
4. Na página **Adicionar conexão**, forneça valores para os campos e selecione **OK.**



A conexão é estabelecida entre seu circuito ExpressRoute e sua rede virtual:



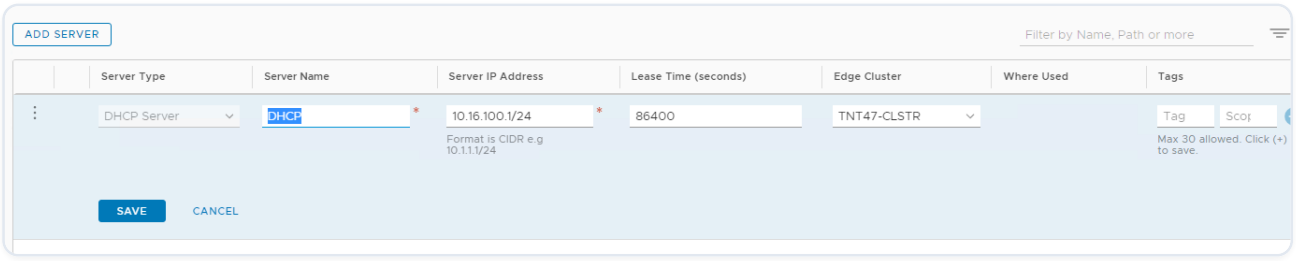
CONFIGURAR DHCP PARA AZURE VMWARE SOLUTION

Após conectar o ExpressRoute ao gateway virtual, configure o DHCP.

Use o NSX-T para hospedar seu servidor DHCP

No NSX-T Manager:

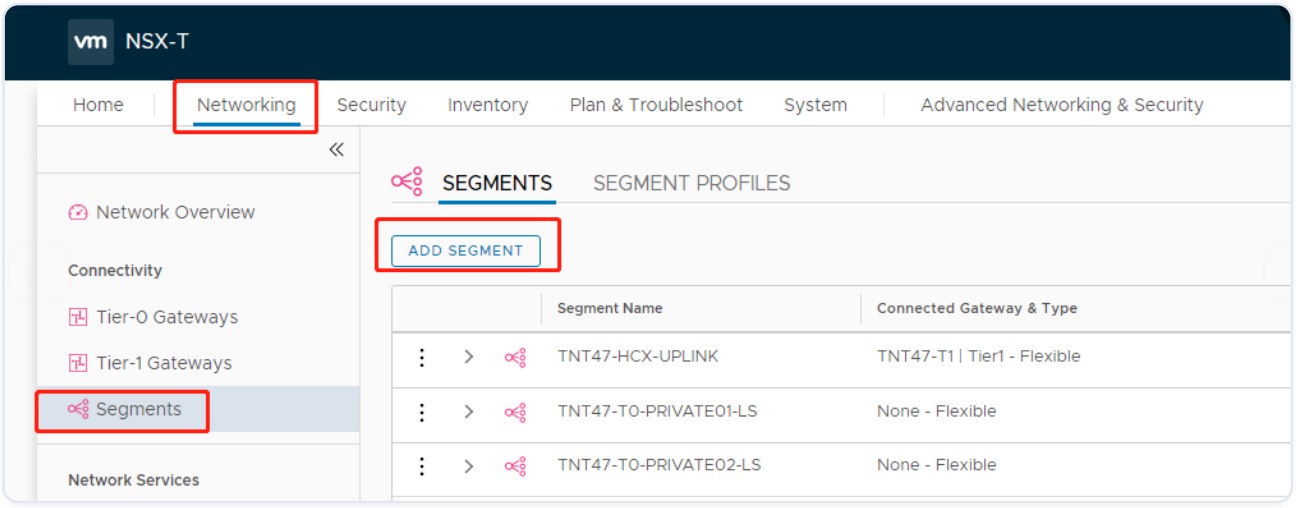
1. Selecione **Rede > DHCP** e então selecione **Adicionar Servidor**.
2. Selecione **DHCP** para o **Tipo de Servidor**, forneça o nome do servidor e o endereço IP.
3. Clique em **Salvar**.
4. Selecione **Gateways de Camada 1**, selecione as reticências verticais no gateway de Camada 1 e então selecione **Editar**.
5. Selecione **Nenhum Conjunto de Alocação de IP** para adicionar uma sub-rede.
6. Selecione **Servidor DHCP Local** para o **Tipo**.
7. Para o **Servidor DHCP**, selecione **DHCP Padrão** e então clique em **Salvar**.
8. Clique em **Salvar** novamente e, em seguida, selecione **Fechar Edição**.



ADICIONAR UM SEGMENTO DE REDE NA SOLUÇÃO AZURE VMWARE

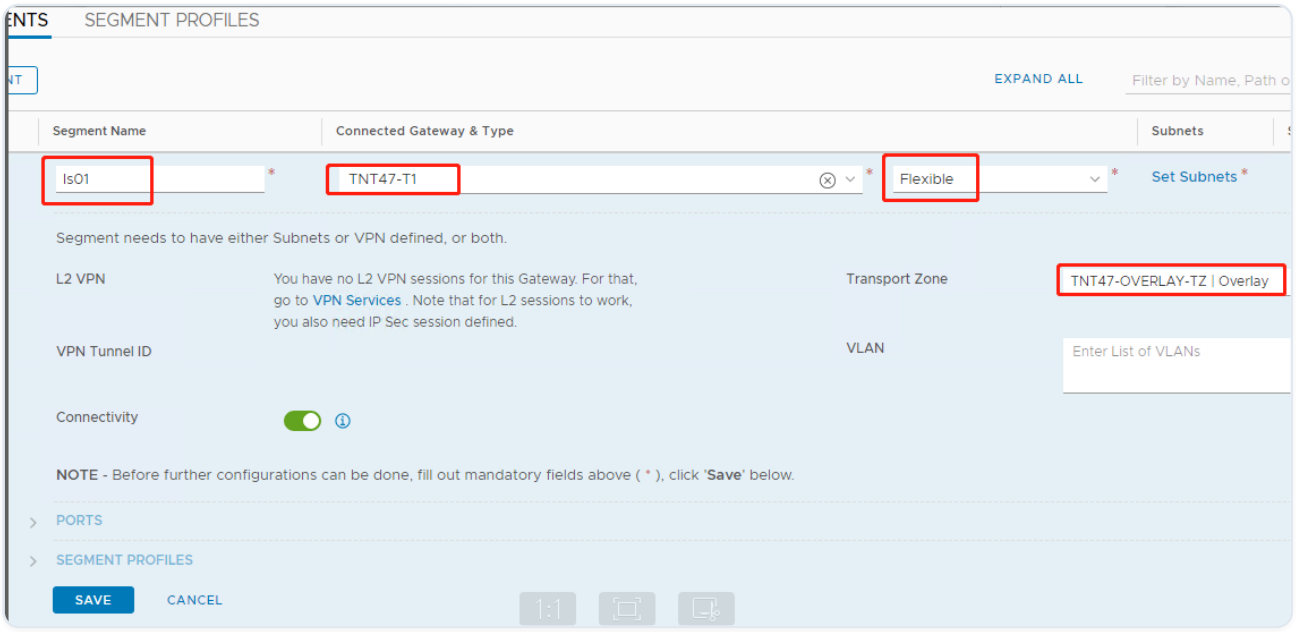
Após configurar o DHCP, adicione um segmento de rede.

Para adicionar um segmento de rede, no NSX-T Manager, selecione **Rede > Segmentos** e, em seguida, clique em **Adicionar Segmento**.



Na tela **Perfil de segmentos**:

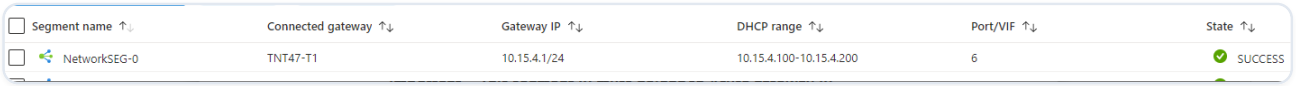
1. Insira um **nome** para o segmento.
2. Selecione o **Gateway Tier-1 (TNTxx-T1)** como o **Gateway Conectado** e deixe o **Tipo** como **Flexível**.
3. Selecione a **Zona de Transporte (TNTxx-OVERLAY-TZ)** de sobreposição pré-configurada.
4. Clique em **Definir Sub-redes**.



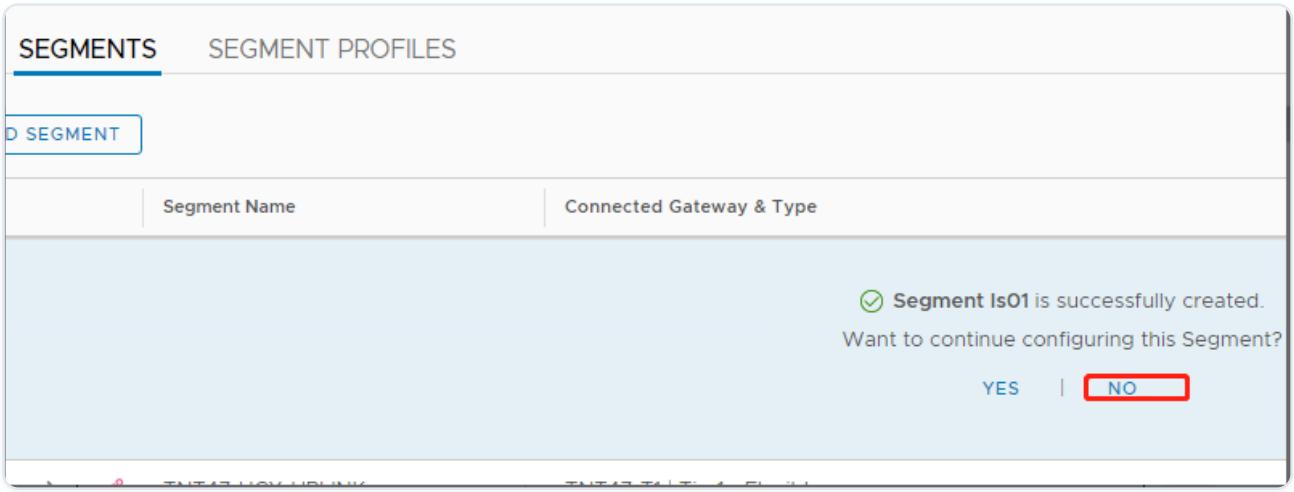
Na seção **Sub-redes**:

1. Insira o endereço IP do gateway.
2. Selecione **Adicionar**.

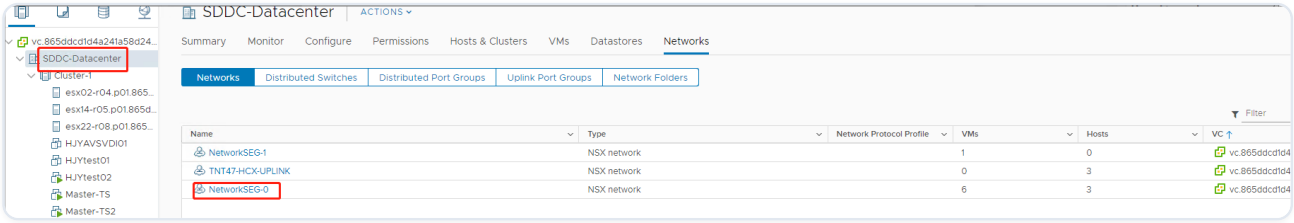
> **Importante:**
>
> Este endereço IP de segmento deve pertencer ao endereço IP do gateway do Azure, 10.15.0.0/22.
>
> O intervalo DHCP deve pertencer ao endereço IP do segmento:



Selecione **Não** para recusar a opção de continuar configurando o segmento:



No vCenter, selecione **Networking > SDDC-Datacenter**:



VERIFICAR O AMBIENTE AVS

Configure o local do recurso para a nuvem privada AVS e instale um par de conectores de nuvem.

CRIAR A CONEXÃO AVS NO CITRIX STUDIO

1. Crie uma máquina no vCenter e instale um par de Cloud Connectors na máquina. Consulte Configurar as instâncias.
2. No Studio, selecione Hosting no painel esquerdo.
3. Selecione o nó de hospedagem e clique em **Adicionar Conexão e Recursos**.
4. Na tela **Conexão**, selecione **Criar uma nova Conexão** e os seguintes detalhes:

   Adicionar Conexão e Recursos(/en-us/citrix-daas/media/avs-vmware-add-connection.png)

   a. Selecione **Tipo de conexão** como **VMware vSphere**.
   b. Em **Endereço de conexão**, insira o endereço IP privado do vCenter.
   c. Insira as credenciais do vCenter.
   d. Insira um nome de conexão.
   e. Escolha a ferramenta para criar máquinas virtuais.

5. Na tela **Rede**, selecione a sub-rede criada no servidor NSX-T.
6. Conclua o assistente.

Google Cloud VMware Engine

O Citrix DaaS permite migrar cargas de trabalho Citrix locais baseadas em VMware para o Google Cloud VMware Engine.

Configurar o Google Cloud VMware Engine

O procedimento a seguir descreve como adquirir e configurar um cluster no Google Cloud VMware Engine.

ACESSAR O PORTAL DO VMWARE ENGINE

1. No **Google Cloud Console**, clique no menu de navegação.
2. Na seção **Compute**, clique em **VMware Engine** para abrir o VMware Engine em uma nova guia do navegador.

REQUISITOS PARA CRIAR A PRIMEIRA NUVEM PRIVADA

Você deve ter acesso ao Google Cloud VMware Engine, cota de nó do VMware Engine disponível e uma função IAM apropriada. Configure os seguintes requisitos antes de continuar a criar sua nuvem privada:

1. Solicite acesso à API e cota de nó. Para obter mais informações, consulte Solicitando acesso à API e cota.
2. Anote os intervalos de endereço que você deseja usar para os dispositivos de gerenciamento VMware e a rede de implantação HCX. Para obter mais informações, consulte Requisitos de rede.

   > **Observação:**
   >
   > A implantação do HCX é aplicável apenas à versão 1.0 do Plano de IP.

3. Obtenha a função IAM de Administrador de Serviço do VMware Engine.

CRIE SUA PRIMEIRA NUVEM PRIVADA

1. Acesse o portal do VMware Engine.
2. Na página inicial do VMware Engine, clique em **Criar uma nuvem privada**. O local de hospedagem e os tipos de nó de hardware são listados.
3. Selecione o número de nós para a nuvem privada. Pelo menos três nós são necessários.

4. Insira um intervalo de Roteamento Entre Domínios Sem Classe (CIDR) para a rede de gerenciamento VMware.
5. Insira um intervalo CIDR para a rede de implantação HCX.

> **Importante:**
>
> - O intervalo CIDR não deve se sobrepor a nenhuma de suas sub-redes locais ou na nuvem. O intervalo CIDR deve ser /27 ou superior.
> - A implantação do HCX é aplicável apenas à versão 1.0 do Plano de IP.

6. Selecione **Revisar e criar**.
7. Revise as configurações. Para alterar qualquer configuração, clique em **Voltar**.
8. Clique em **Criar** para começar a criar a nuvem privada.

À medida que o VMware Engine cria sua nova nuvem privada, ele implanta vários componentes VMware e configura políticas iniciais de Autoscale™ para clusters na nuvem privada. A criação da nuvem privada pode levar de 30 minutos a 2 horas. Após a conclusão do provisionamento, você receberá um e-mail.

CONFIGURAR O GATEWAY VPN DO GOOGLE CLOUD VMWARE ENGINE

Para estabelecer uma conectividade inicial com o Google Cloud VMware Engine, você pode usar um gateway VPN. Este é um VPN de cliente baseado em OpenVPN, através do qual você pode se conectar ao seu vCenter do VMware Software Defined Data Center (SDDC) e realizar qualquer configuração inicial necessária.

Antes de implantar um gateway VPN, configure o intervalo de **Serviços de Borda** para a região onde seu SDDC está implantado. Para fazer isso:

1. Faça login no portal **Google Cloud VMware Engine** e vá para **Rede > Configurações Regionais**. Clique em **Adicionar Região**.
2. Escolha a região onde seu SDDC está implantado e habilite **Acesso à Internet** e **Serviço de IP Público**.
3. Forneça o intervalo de Serviços de Borda anotado durante o planejamento e clique em **Enviar**. A habilitação desses serviços leva de 10 a 15 minutos.

Uma vez concluído, os Serviços de Borda aparecem como **Habilitados** na página Configurações Regionais. A habilitação dessas configurações permite que IPs Públicos sejam alocados ao seu SDDC, o que é um requisito para implantar um gateway VPN.

Implantar um gateway VPN

1. No portal **Google Cloud VMware Engine**, vá para **Rede > Gateways VPN**. Clique em **Criar Novo Gateway VPN**.
2. Forneça o nome para o gateway VPN e a sub-rede do cliente reservada durante o planejamento. A localização da VPN deve ser a mesma da região da nuvem privada. Clique em **Avançar**.
3. Selecione os usuários para conceder acesso VPN. Clique em **Avançar**.
4. Especifique as redes que devem ser acessíveis via VPN. Clique em **Avançar**.
5. Uma tela de resumo é exibida. Verifique as seleções e clique em **Enviar** para criar o Gateway VPN. A página Gateways VPN é exibida com o status do novo gateway VPN como **Criando**.
6. Depois que o status mudar para **Operacional**, clique no novo gateway VPN.
7. Clique em **Baixar minha configuração VPN** para baixar um arquivo ZIP contendo perfis OpenVPN pré-configurados para o gateway VPN. Perfis para conexão via UDP/1194 e TCP/443 estão disponíveis. Escolha sua preferência e importe-a para o Open VPN e, em seguida, conecte-se.
8. Vá para **Recursos** e selecione seu SDDC.

CONECTAR A VPN

1. Estabeleça uma conexão ponto a site entre sua rede local e a nuvem privada por meio da configuração do Gateway VPN. Consulte Configurar o Gateway VPN do Google Cloud VMware Engine.
2. Carregue a configuração VPN baixada em Configurar o Gateway VPN do Google Cloud VMware Engine.
3. Importe para seu cliente VPN, por exemplo, OpenVPN Connect.

Para obter mais informações, consulte Conectando usando VPN.

CRIAR PRIMEIRA SUB-REDE

Acessar o NSX-T Manager no portal do VMware Engine
O processo de criação de uma sub-rede ocorre no NSX-T, que você acessa por meio do VMware Engine. Faça o seguinte para acessar o NSX-T Manager.

1. Faça logon no portal **Google Cloud VMware Engine**.

2. Na navegação principal, vá para **Recursos**.
3. Clique no **nome da nuvem privada** correspondente à nuvem privada onde você deseja criar a sub-rede.
4. Na página de detalhes da sua nuvem privada, clique na guia **vSphere Management Network**.
5. Clique no **FQDN** correspondente ao NSX-T Manager.
6. Quando solicitado, insira suas credenciais de login. Se você configurou o vIDM e o conectou a uma fonte de identidade, como o Active Directory, use suas credenciais de fonte de identidade.

> **Lembrete:**
>
> Você pode recuperar as credenciais geradas na página de detalhes da nuvem privada.

Configurar o serviço DHCP para a sub-rede
Antes de criar uma sub-rede, configure um serviço DHCP:

No NSX-T Manager:

1. Vá para **Rede > DHCP**. O painel de rede mostra que o serviço DHCP cria um gateway Tier-0 e um gateway Tier-1.
2. Para começar a provisionar um servidor DHCP, clique em **Adicionar Servidor**.
3. Selecione **DHCP** para o **Tipo de Servidor**, forneça o nome do servidor e o endereço IP.
4. Clique em **Salvar** para criar o serviço DHCP.

Faça o seguinte para anexar este serviço DHCP ao gateway Tier-1 relevante. Um gateway Tier-1 padrão já é provisionado pelo serviço DHCP:

1. Selecione **Gateways Tier 1**, selecione as reticências verticais no gateway Tier-1 e, em seguida, selecione **Editar**.
2. No campo **Gerenciamento de Endereços IP**, selecione **Nenhum Conjunto de Alocação de IP**.
3. Selecione **Servidor DHCP Local** para o **Tipo**.
4. Selecione o servidor DHCP que você criou para o **Servidor DHCP**.
5. Clique em **Salvar**.
6. Clique em **Fechar Edição**.

Agora você pode criar um segmento de rede no NSX-T. Para obter mais informações sobre DHCP no NSX-T, consulte a documentação da VMware para DHCP.

Criar um segmento de rede no NSX-T

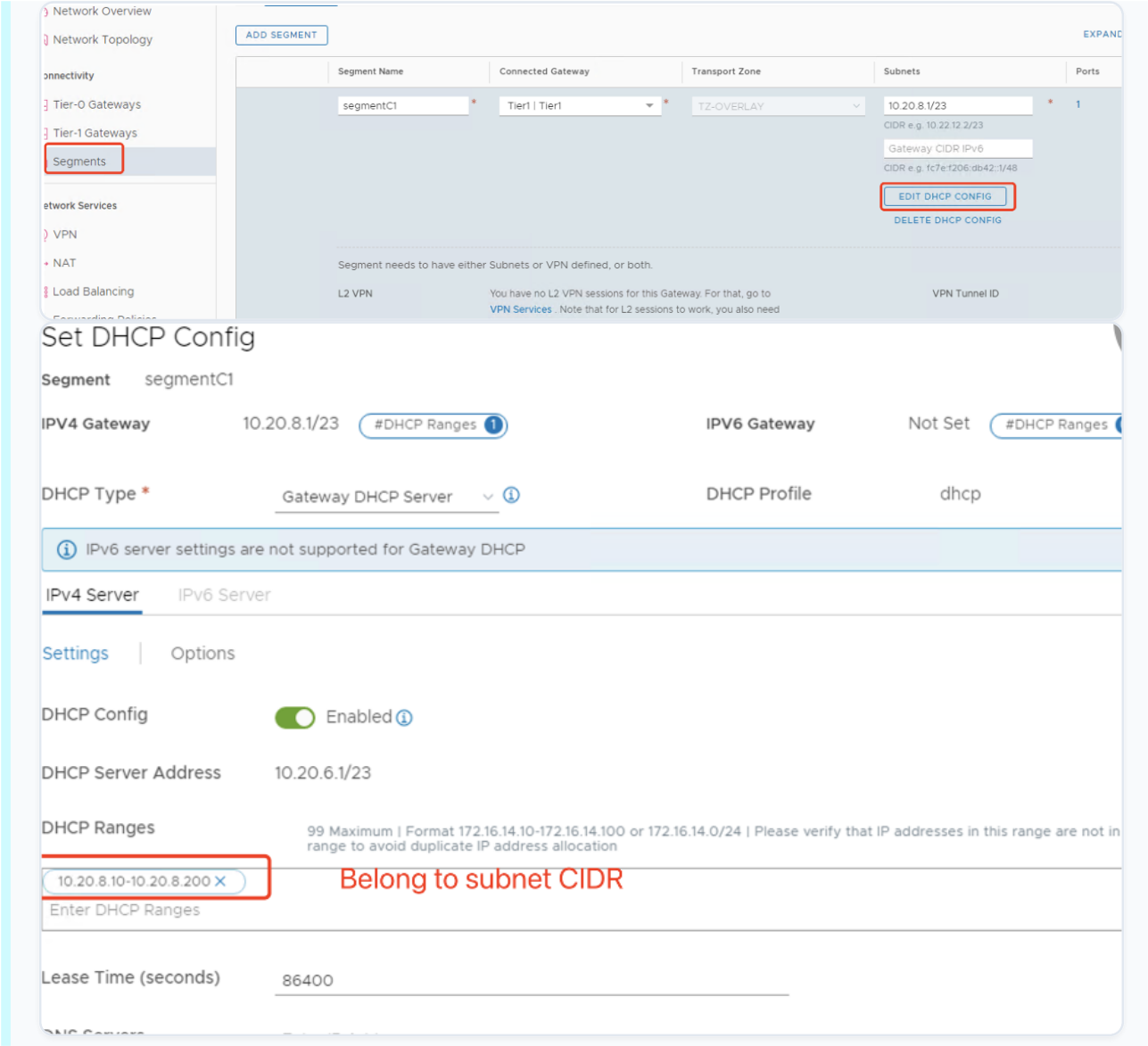
Para VMs de carga de trabalho, você cria sub-redes como segmentos de rede NSX-T para sua nuvem privada:

1. No NSX-T Manager, vá para **Rede > Segmentos**.
2. Clique em **Adicionar Segmento**.
3. Insira um nome para o segmento.
4. Selecione o **Tier-1** como o **Gateway Conectado** e deixe o Tipo como **Flexível**.
5. Clique em **Definir Sub-redes**.
6. Clique em **Adicionar Sub-redes**.
7. Insira o intervalo da sub-rede em **Gateway IP/Prefix Length**. Especifique o intervalo da sub-rede com **.1** como o último octeto. Por exemplo, **10.12.2.1/24**.
8. Especifique os intervalos DHCP e clique em **ADD**.
9. Em **Transport Zone**, selecione **TZ-OVERLAY** na lista suspensa.
10. Clique em **Salvar**. Agora você pode selecionar este segmento de rede no vCenter ao criar uma VM.

Em uma determinada região, você pode configurar no máximo 100 rotas exclusivas do VMware Engine para sua rede VPC usando acesso a serviços privados. Isso inclui, por exemplo, intervalos de endereços IP de gerenciamento de nuvem privada, segmentos de rede de carga de trabalho NSX-T e intervalos de endereços IP de rede HCX. Este limite inclui todas as nuvens privadas na região.

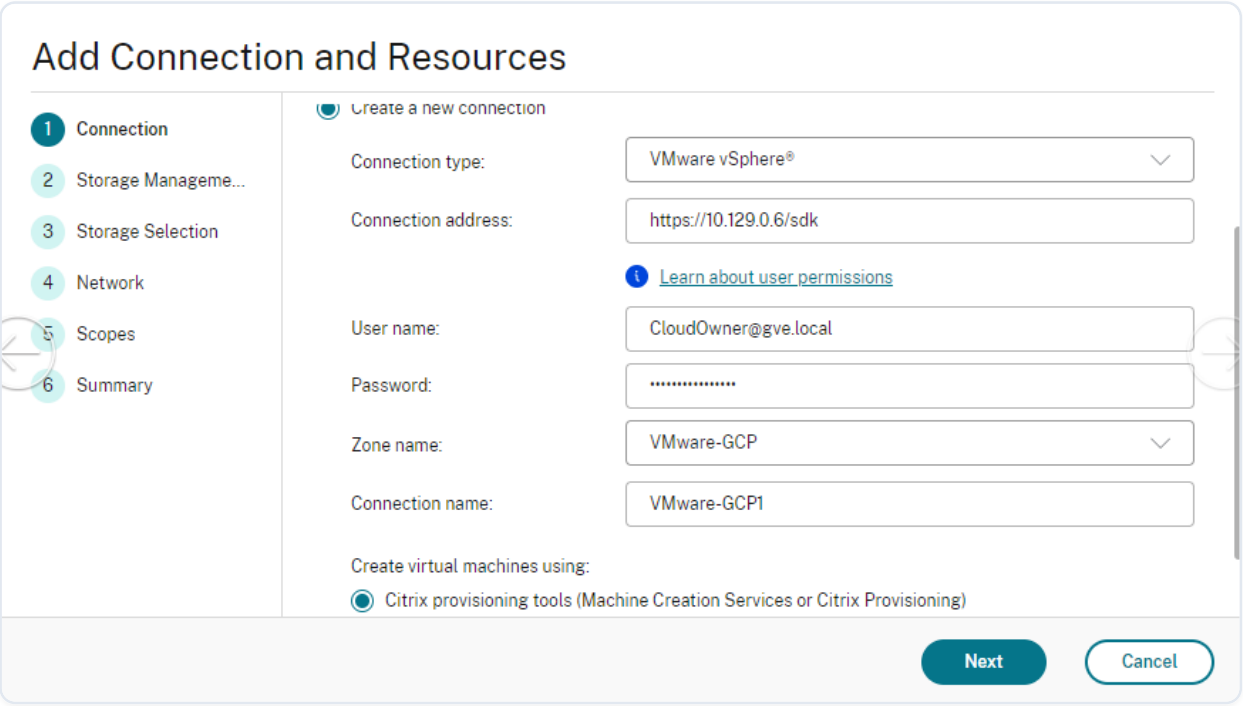
> **Nota:**

> Há um problema de configuração do Google Cloud devido ao qual você precisa configurar a definição do intervalo DHCP várias vezes. Portanto, certifique-se de configurar a definição do intervalo DHCP após a configuração do Google Cloud. Clique em **EDIT DHCP CONFIG** para configurar os intervalos DHCP.



CRIAR A CONEXÃO GOOGLE CLOUD VMWARE NO CITRIX STUDIO

1. Crie uma máquina no vCenter e instale um par de Cloud Connectors na máquina. Consulte Configurar as instâncias.
2. Inicie o Citrix Studio.
3. Selecione o nó de hospedagem e clique em **Adicionar Conexão e Recursos**.
4. Na tela **Conexão**, selecione **Criar uma nova Conexão** e os seguintes detalhes:



a. Selecione **Tipo de conexão** como **VMware vSphere**.

b. No **Endereço de conexão**, insira o endereço IP privado do vCenter.

c. Insira as credenciais do vCenter.

d. Insira um nome de conexão.

e. Escolha a ferramenta para criar máquinas virtuais.

5. Na tela **Rede**, selecione a sub-rede criada no servidor NSX-T.
6. Conclua o assistente.

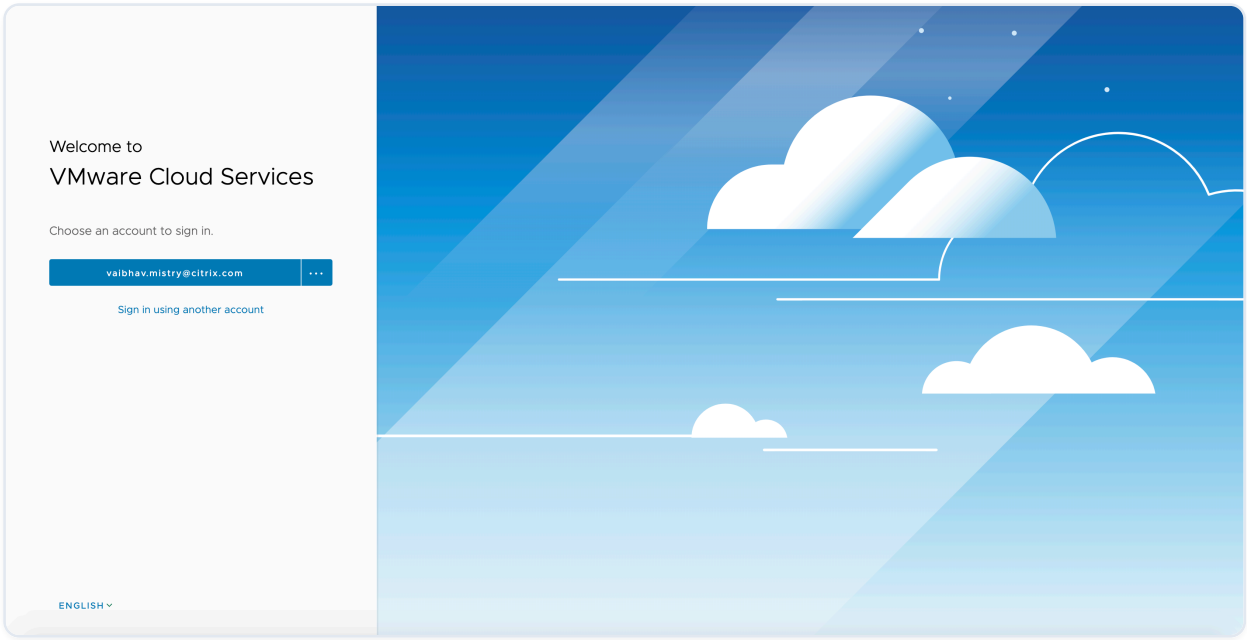
VMware Cloud no Amazon Web Services (AWS)

O VMware Cloud no Amazon Web Services (AWS) permite migrar cargas de trabalho Citrix locais baseadas em VMware para o AWS Cloud e seu ambiente principal do Citrix Virtual Apps and Desktops para o Citrix DaaS.

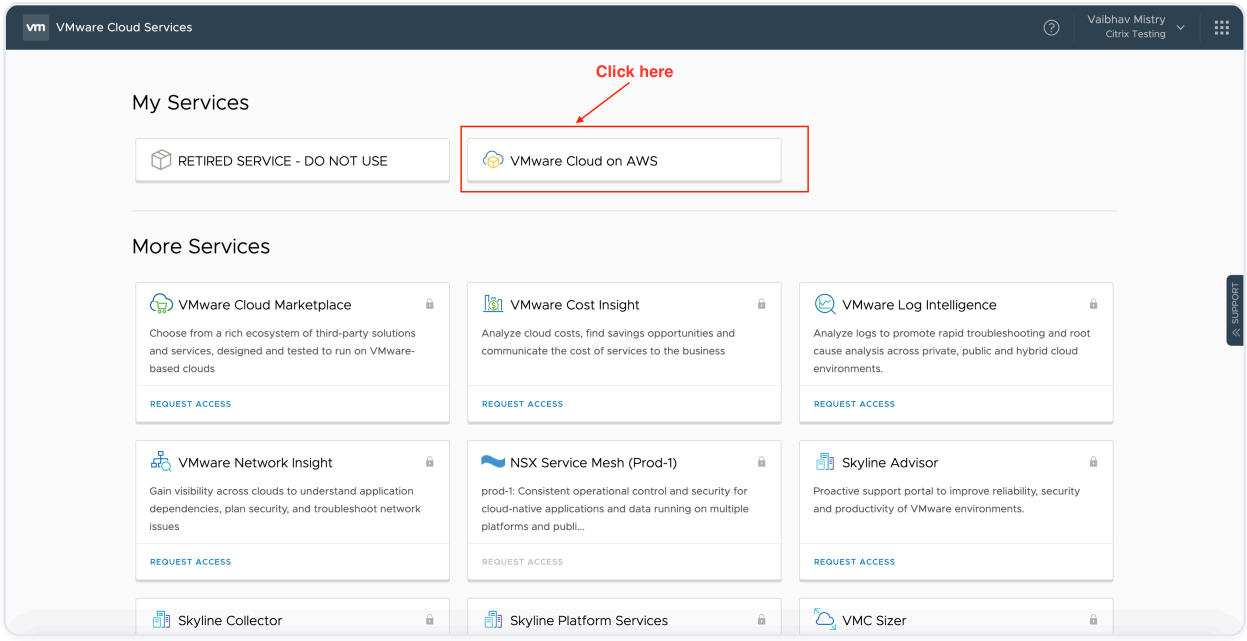
Este artigo descreve o procedimento para configurar um VMware Cloud no AWS.

Acessar o ambiente VMware Cloud

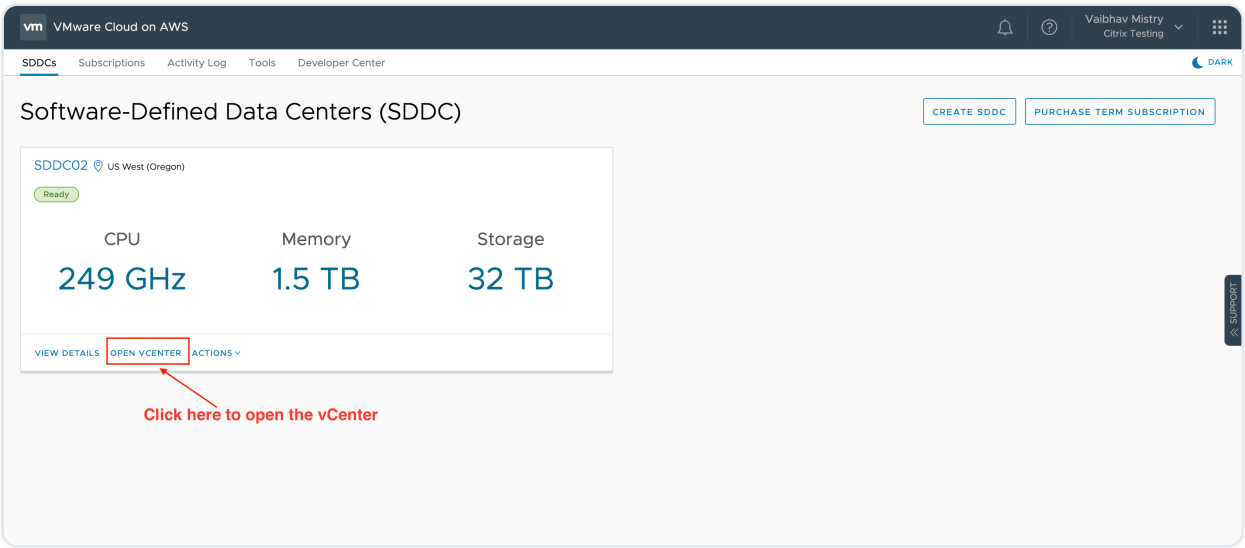
1. Faça login nos serviços de nuvem VMware usando o URL `<https://console.cloud.vmware.com/>`.

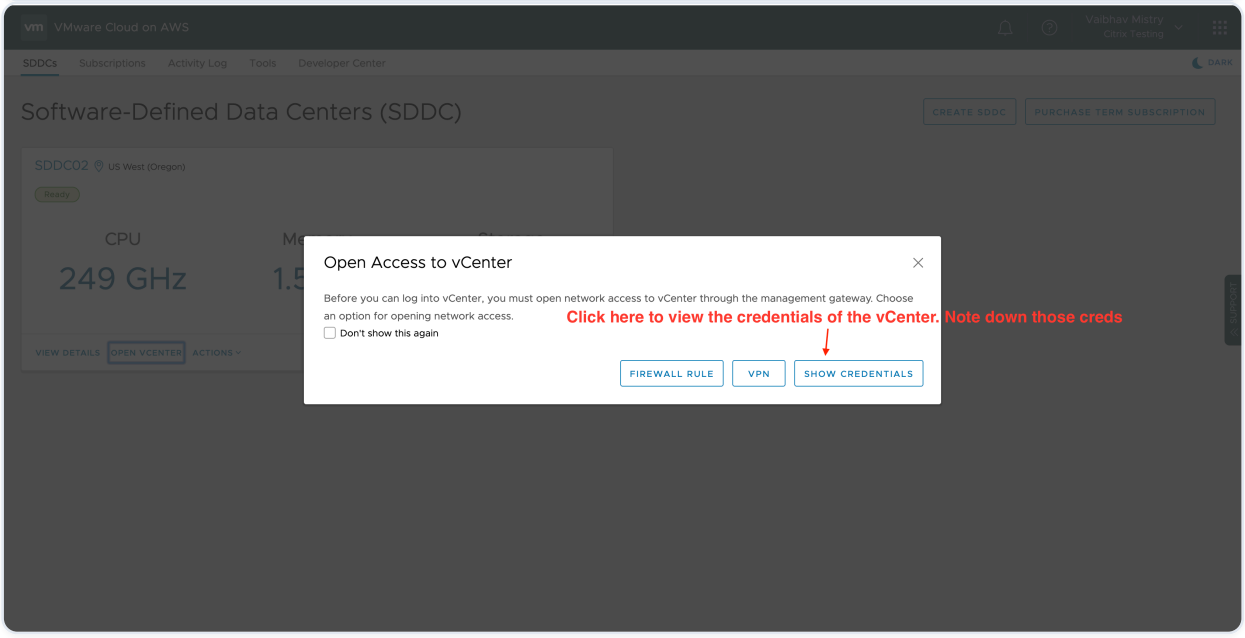


2. Clique em **VMware Cloud on AWS**. A página Software-Defined Data Centers (SDDC) é exibida.

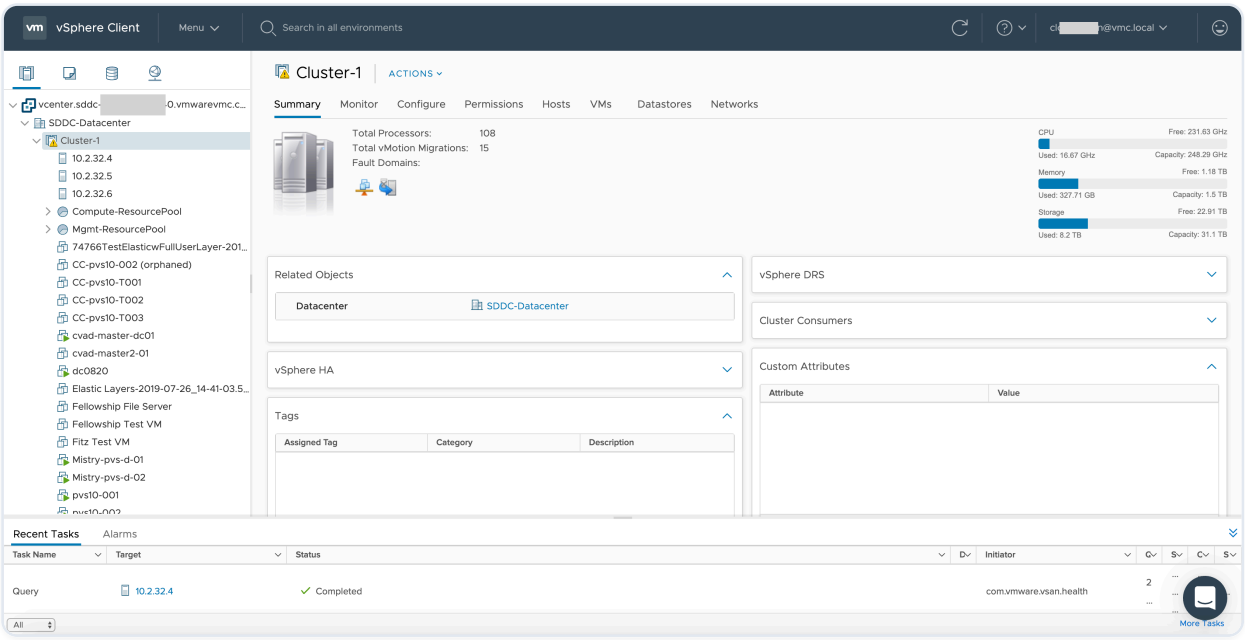


3. Clique em **OPEN VCENTER** e, em seguida, clique em **SHOW CREDENTIALS**. Anote as credenciais para uso posterior.





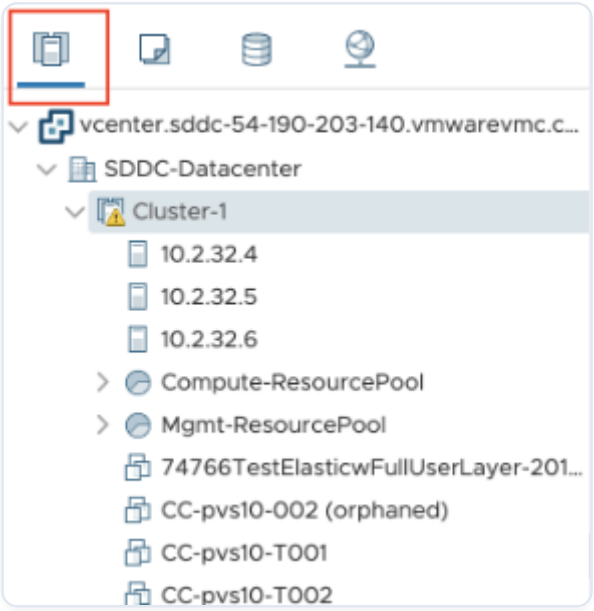
4. Abra um navegador da Web e insira o URL do vSphere Web Client.
5. Insira as credenciais conforme observado e clique em **Login**. A página da Web do cliente vSphere é semelhante ao ambiente local.



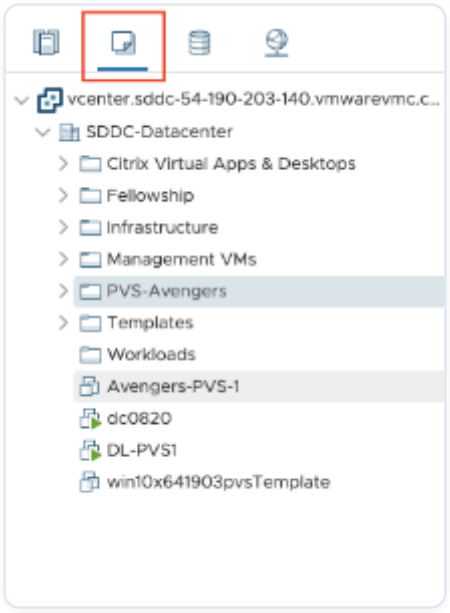
Sobre o ambiente de nuvem VMware

Existem quatro visualizações na página da Web do cliente vSphere.

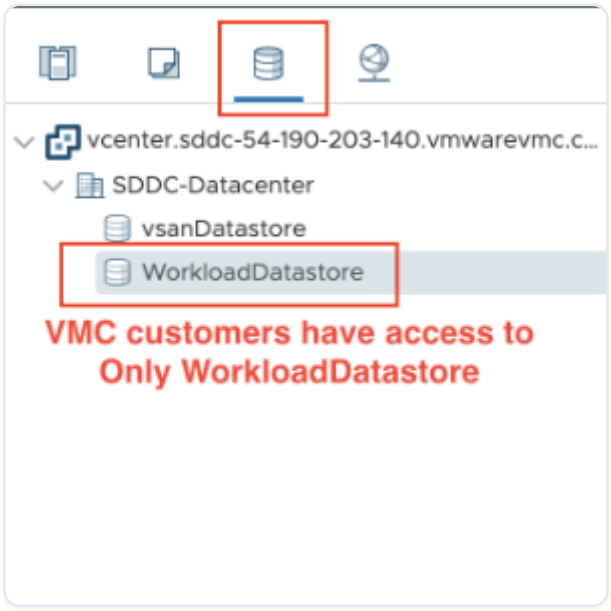
- Visualização de Host e Cluster: Você não pode criar um novo Cluster, mas o administrador da nuvem pode criar vários pools de recursos.



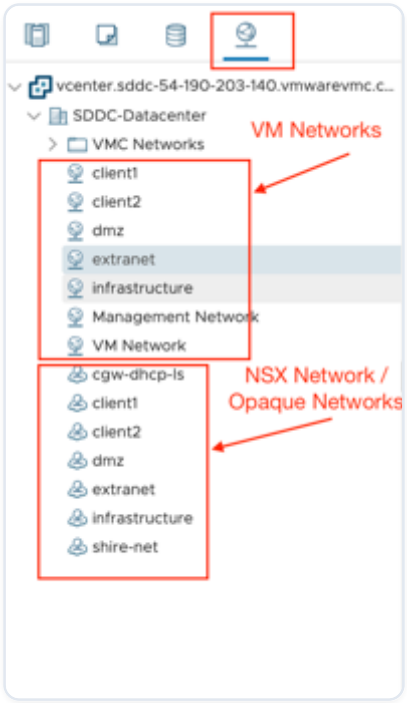
- Visualização de VM e Modelo: O administrador da nuvem pode criar muitas pastas.



- Visualização de Armazenamento: Selecione o armazenamento **WorkloadDatastore** ao adicionar a unidade de hospedagem no Citrix Studio porque você tem acesso apenas ao Workload Datastore.



- Visualização de Rede: Os ícones são diferentes para redes de nuvem VMware e redes opacas.



Depois de configurar o cluster, consulte Ambientes de virtualização VMware para adicionar conexões e recursos.

Próximos passos

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina designada para entregar aplicativos ou um desktop aos seus usuários.
- Para criar e gerenciar uma conexão, consulte Conexão com soluções de nuvem e parceiros VMware.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Ambientes de virtualização XenServer®

O XenServer simplifica seu gerenciamento operacional ao mesmo tempo em que garante uma experiência de usuário de alta definição para cargas de trabalho intensivas.

Para configurar seu XenServer, consulte Adicionar um tipo de recurso.

Próximos passos

- Para uma implantação simples de prova de conceito, instale um VDA em uma máquina designada para entregar aplicativos ou um desktop aos seus usuários.
- Para criar e gerenciar conexões, consulte Conexão ao XenServer.
- Revise todas as etapas do processo de instalação e configuração.

Mais informações

- Criar e gerenciar conexões e recursos
- Criar catálogos de máquinas

Considerações de tamanho e escala para Cloud Connectors

Ao avaliar o Citrix DaaS para dimensionamento e escalabilidade, considere todos os componentes. Pesquise e teste a configuração dos Citrix Cloud™ Connectors e do StoreFront para seus requisitos específicos. Fornecer recursos insuficientes para dimensionamento e escalabilidade afeta negativamente o desempenho da sua implantação.

> **Nota:**
>
> - Estas recomendações se aplicam ao Citrix DaaS Standard for Azure além do Citrix DaaS.
> - Os testes e recomendações fornecidos neste artigo são diretrizes para ajudar você a iniciar seus testes. Recomendamos que você realize os testes em seu ambiente para validar o dimensionamento correto do conector.
> - Para considerações de dimensionamento e escala para proxy HDX, consulte Considerações de dimensionamento e escala do Cloud Connector para proxy HDX.

> Este artigo fornece detalhes das capacidades máximas testadas e recomendações de melhores práticas para a configuração da máquina do Cloud Connector. Os testes foram realizados em implantações configuradas com StoreFront™ e Local Host Cache (LHC).

As informações fornecidas se aplicam a implantações nas quais cada local de recurso contém cargas de trabalho VDI e cargas de trabalho RDS.

O Cloud Connector vincula suas cargas de trabalho ao Citrix DaaS™ das seguintes maneiras:

- Fornece um proxy para comunicação entre seus VDAs e o Citrix DaaS.
- Fornece um proxy para comunicação entre o Citrix DaaS e seu Active Directory (AD) e hypervisors.
- Em implantações que incluem servidores StoreFront, o Cloud Connector atua como um session broker temporário durante interrupções na nuvem, fornecendo aos usuários acesso contínuo aos recursos.

É importante que seus Cloud Connectors sejam dimensionados e configurados adequadamente para atender às suas necessidades específicas. Embora os testes tenham sido executados com dois Cloud Connectors, apenas um Cloud Connector está disponível durante as atualizações do Cloud Connector. Para garantir alta disponibilidade durante as atualizações do Cloud Connector, alguns clientes optaram por implantar três Cloud Connectors.

Cada conjunto de Cloud Connectors é atribuído a um local de recurso (também conhecido como zona no Studio). Um local de recurso é uma separação lógica que especifica quais recursos se comunicam com esse conjunto de Cloud Connectors. Pelo menos um local de recurso é necessário por domínio para se comunicar com o Active Directory (AD).

Cada catálogo de máquinas e conexão de hospedagem é atribuído a um local de recurso.

Para implantações com mais de um local de recurso, atribua catálogos de máquinas e VDAs aos locais de recurso para otimizar a capacidade do LHC de intermediar conexões durante interrupções. Para obter mais informações sobre como criar e gerenciar locais de recurso, consulte Conectar ao Citrix Cloud. Para um desempenho ideal, configure seus Cloud Connectors em conexões de baixa latência com VDAs, servidores AD e hipervisores.

Processadores e armazenamento recomendados

Para um desempenho semelhante ao observado nestes testes, use processadores modernos que suportam extensões SHA. As extensões SHA reduzem a carga criptográfica na CPU. Os processadores recomendados incluem:

- Processadores Advanced Micro Devices (AMD) Zen e mais recentes
- Processadores Intel Ice Lake e mais recentes

Os processadores recomendados funcionam de forma eficiente. Você pode usar processadores mais antigos, no entanto, isso pode levar a uma carga de CPU mais alta. Recomendamos aumentar sua contagem de vCPUs para compensar esse comportamento.

Os testes descritos neste artigo foram realizados com processadores AMD EPYC e Intel Cascade Lake.

Os Cloud Connectors têm uma carga criptográfica pesada ao se comunicar com a nuvem. Cloud Connectors que usam processadores com extensões SHA experimentam uma carga menor em sua CPU, o que é expresso por um menor uso da CPU pelo Serviço de Subsistema da Autoridade de Segurança Local do Windows (LSASS).

A Citrix recomenda o uso de armazenamento moderno com operações de E/S por segundo (IOPS) adequadas, especialmente para implantações que usam LHC. Unidades de estado sólido (SSDs) são sugeridas, mas camadas de armazenamento em nuvem premium não são necessárias. IOPS mais altos são necessários para cenários de LHC onde o Cloud Connector executa uma pequena cópia do banco de dados. Este banco de dados é atualizado regularmente com alterações de configuração do site e fornece recursos de intermediação para o local de recurso em tempos de interrupções do Citrix Cloud.

Configuração de computação recomendada para Local Host Cache

O Local Host Cache (LHC) oferece alta disponibilidade, permitindo que as operações de intermediação de conexão em uma implantação continuem quando um Cloud Connector não consegue se comunicar com o Citrix Cloud.

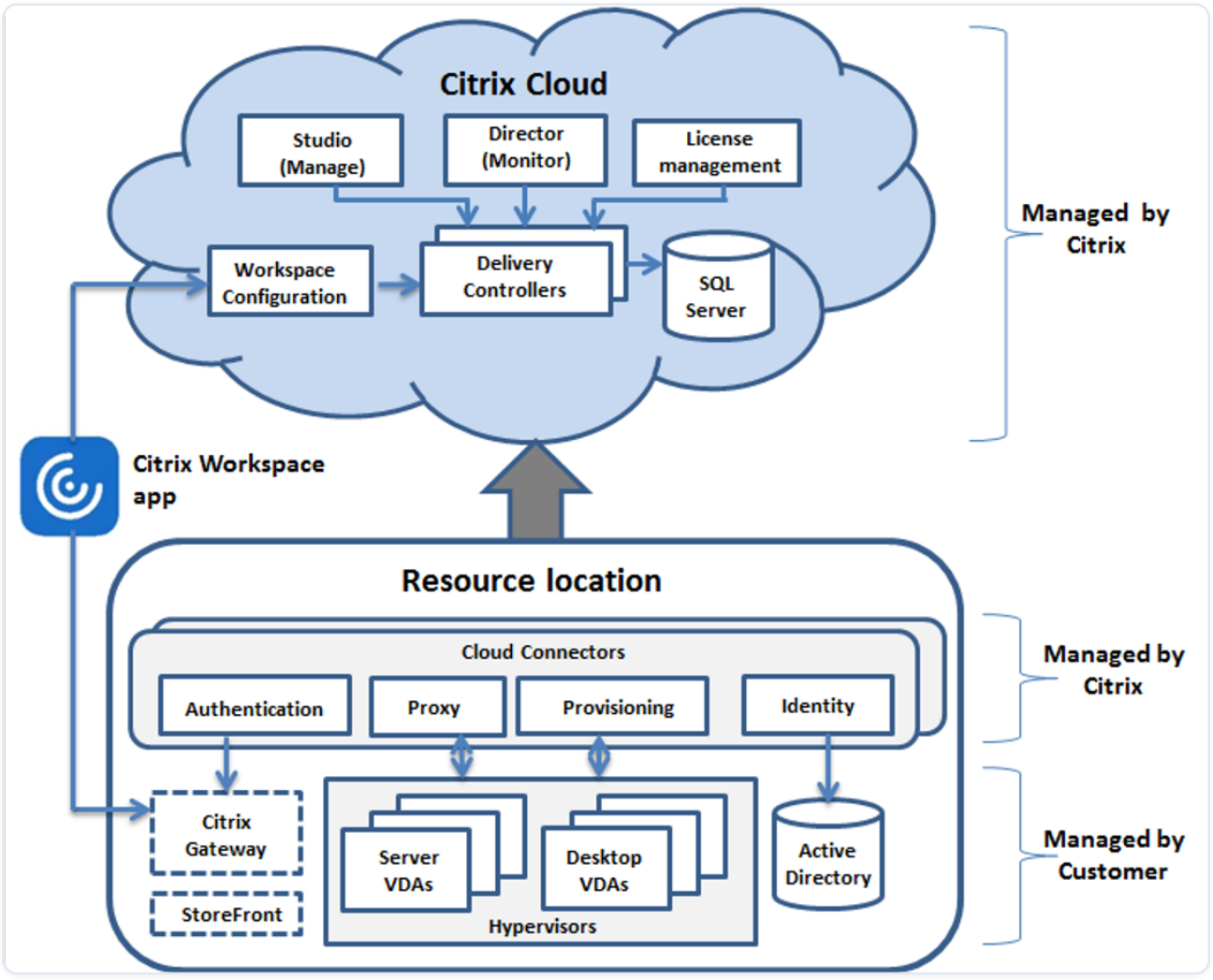
Os Cloud Connectors executam o Microsoft SQL Express Server LocalDB, que é instalado automaticamente quando você instala o Cloud Connector. A configuração da CPU do Cloud Connector, especialmente o número de núcleos disponíveis para o SQL Express Server LocalDB, afeta diretamente o desempenho do LHC. O número de núcleos de CPU disponíveis para o SQL Server Express Server LocalDB afeta o desempenho do LHC ainda mais do que a alocação de memória. Essa sobrecarga da CPU é observada apenas no modo LHC quando o Citrix DaaS não está acessível e o broker LHC está ativo. Para qualquer implantação que use LHC, a Citrix recomenda quatro núcleos por soquete, com um mínimo de quatro núcleos de CPU por Cloud Connector. Para obter informações sobre como configurar recursos de computação para o SQL Express Server LocalDB, consulte Limites de capacidade de computação por edição do SQL Server.

Se os recursos de computação disponíveis para o SQL Express Server LocalDB estiverem configurados incorretamente, os tempos de sincronização da configuração podem ser aumentados e o desempenho durante interrupções pode ser reduzido. Em alguns ambientes virtualizados, a capacidade de computação pode depender do número de processadores lógicos e não de núcleos de CPU.

Resumo dos resultados dos testes

Todos os resultados neste resumo são baseados nas descobertas de um ambiente de teste conforme configurado nas seções detalhadas deste artigo. Os resultados mostrados aqui são para um único local de recurso. Diferentes configurações de sistema podem produzir resultados diferentes.

Esta ilustração oferece uma visão geral gráfica da configuração testada.



A tabela a seguir mostra as configurações mínimas recomendadas de CPU e memória do Cloud Connector para sites de vários tamanhos. Os resultados dos testes com essas configurações são mostrados abaixo. Consulte Limites para obter mais informações sobre os limites de localização de recursos.

	MÉDIO	GRANDE	MÁXIMO
Conectores para HA	2	2	3
VDAs	Até 1000	1001 - 5000	5001 - 10.000

	MÉDIO	GRANDE	MÁXIMO
Sessões	Até 2500	Até 10.000	Até 25.000
Conexões de hospedagem	Até 20	Até 40	Até 40
CPUs para Cloud Connectors	4vCPU	4vCPU	8vCPU
Memória para Cloud Connectors	6 GB	8 GB	10 GB

> **Observação:**
>
> Se sua implantação exceder 5000 VDAs, você deve usar três Cloud Connectors para alta disponibilidade e escalabilidade.

Metodologia de teste

Testes foram realizados para adicionar carga e medir o desempenho dos componentes do ambiente. Os componentes foram monitorados coletando dados de desempenho e tempo de procedimento, como tempo de logon e tempo de registro. Às vezes, ferramentas de simulação proprietárias da Citrix são usadas para simular VDAs e sessões. Essas ferramentas são projetadas para exercitar os componentes da Citrix da mesma forma que os VDAs e sessões tradicionais, sem os mesmos requisitos de recursos para hospedar sessões e VDAs reais. Os testes foram realizados nos modos de corretagem em nuvem e LHC para cenários com Citrix StoreFront.

As recomendações para o dimensionamento do Cloud Connector neste artigo são baseadas em dados coletados desses testes.

Os seguintes testes foram executados:

- **Tempestade de logon/inicialização de sessão:** um teste que simula períodos de logon de alto volume.
- **Tempestade de registro de VDA:** um teste que simula períodos de registro de VDA de alto volume. Por exemplo, após um ciclo de atualização ou transição entre o modo de corretagem em nuvem e o modo Local Host Cache.

- **Tempestade de ação de energia de VDA:** um teste que simula alto volume de ações de energia de VDA.

Cenários e condições de teste

Esses testes foram realizados com o LHC configurado. Para obter mais informações sobre o uso do LHC, consulte o artigo Local Host Cache. O LHC requer um servidor StoreFront local. Para obter informações detalhadas sobre o StoreFront, consulte a documentação do produto StoreFront.

Recomendações para configurações do StoreFront:

- Se você tiver vários locais de recursos com um único servidor StoreFront ou grupo de servidores, habilite a opção de verificação de integridade avançada para o armazenamento do StoreFront. Consulte Requisito do StoreFront no artigo Local Host Cache.
- Para taxas de inicialização de sessão mais altas, use um grupo de servidores StoreFront. Consulte Configurar grupos de servidores na documentação do produto StoreFront.

Condições de teste:

- Os requisitos de CPU e memória são apenas para o SO base e serviços Citrix. Aplicativos e serviços de terceiros podem exigir recursos adicionais.
- VDAs são quaisquer máquinas virtuais ou físicas executando o Citrix Virtual Delivery Agent.
- Os testes são realizados usando apenas VDAs Windows.
- Todos os VDAs testados foram gerenciados por energia usando o Citrix DaaS.
- As sessões foram iniciadas a uma taxa sustentada de 1.000 por minuto.
- Foram testadas cargas de trabalho de 1.000 a 10.000 VDI e 500 a 10.000 servidores RDS com 1.000 a 25.000 sessões.
- As sessões RDS foram testadas em até 25.000 por local de recurso.
- Os testes foram realizados usando dois Cloud Connectors tanto em operações normais quanto durante uma interrupção. A Citrix recomenda usar pelo menos dois Cloud Connectors para alta disponibilidade e três Cloud Connectors para locais de recurso de tamanho máximo e grande. No modo de interrupção, apenas um dos Cloud Connectors é usado para registros e intermediação de VDA. Embora os testes tenham sido executados com dois Cloud Connectors, apenas um Cloud Connector está disponível durante as atualizações. Para garantir alta disponibilidade durante as atualizações, alguns clientes optaram por operar com três Cloud Connectors.

- Os testes foram realizados com o Cloud Connector configurado com processadores Intel Cascade Lake.
- As sessões foram iniciadas por meio de um único servidor Citrix StoreFront.
- Testes de lançamento de sessões de interrupção do LHC realizados após as máquinas terem sido registradas novamente.

As contagens de sessões RDS são uma recomendação e não um limite. Teste seu próprio limite de sessão RDS em seu ambiente.

> **Nota:**
>
> A contagem de sessões e a taxa de lançamento são mais importantes para RDS do que a contagem de VDAs.

Cargas de trabalho médias

Essas cargas de trabalho foram testadas com 4 vCPUs e 6 GB de memória.

CARGAS DE TRABALHO DE TESTE	CONDIÇÃO DO SITE	TEMPO DE REGISTRO DO VDA	USO DE CPU E MEMÓRIA NO REGISTRO	DURAÇÃO DO TESTE DE INICIALIZAÇÃO	USO DE CPU E MEMÓRIA NA INICIALIZAÇÃO DA SESSÃO	TAXA DE INICIALIZAÇÃO
1000 VDIs	Online	5 minutos	CPU máxima = 36%, CPU média = 33%, memória máxima = 5,3 GB	2 minutos	CPU máxima = 29%, CPU média = 27%, memória máxima = 3,7 GB	500 por minuto
1000 VDI	Interrupção	4 minutos	CPU máxima = 11%, CPU média =	2 minutos	CPU máxima = 42%, CPU média =	500 por minuto

CARGAS DE TRABALHO DE TESTE	CONDIÇÃO DO SITE	TEMPO DE REGISTRO DO VDA	USO DE CPU E MEMÓRIA NO REGISTRO	DURAÇÃO DO TESTE DE INICIALIZAÇÃO	USO DE CPU E MEMÓRIA NA INICIALIZAÇÃO DA SESSÃO	TAXA DE INICIALIZAÇÃO
			10%, memória máxima = 4,5 GB		28%, memória máxima = 4,0 GB	
250 RDS, 5000 sessões	Online	3 minutos	CPU máxima = 14%, CPU média = 4%, memória máxima = 3,5 GB	9 minutos	CPU máxima = 46%, CPU média = 21%, memória máxima = 3,7 GB	555 por minuto
250 RDS, 5000 sessões	Interrupção	3 minutos	CPU máxima = 15%, CPU média = 5%, memória máxima = 3,7	9 minutos	CPU máxima = 51%, CPU média = 32%, memória máxima = 4,2 GB	555 por minuto

Cargas de trabalho grandes

Essas cargas de trabalho foram testadas com 4 vCPUs e 8 GB de memória.

CARGAS DE TRABALHO DE TESTE	CONDIÇÃO DO SITE	TEMPO DE REGISTRO DO VDA	USO DE CPU E MEMÓRIA DE REGISTRO	DURAÇÃO DO TESTE DE INICIALIZAÇÃO	USO DE CPU E MEMÓRIA NA INICIALIZAÇÃO DA SESSÃO	TAXA DE INICIALIZAÇÃO
5000 VDI	Online	3–4 minutos	CPU máxima = 45%, CPU média = 25%, memória máxima = 7,0 GB	5 minutos	CPU máxima = 75%, CPU média = 55%, memória máxima = 7,0 GB	1000 por minuto
5000 VDI	Interrupção	4–6 minutos	CPU máxima = 15%, CPU média = 5%, memória máxima = 7,5 GB	5 minutos	CPU máxima = 45%, CPU média = 40%, memória máxima = 7,5 GB	1000 por minuto
500 RDS, 10.000 sessões	Online	3 minutos	CPU máxima = 45%, CPU média = 25%, memória máxima = 7,0 GB	10 minutos	CPU máxima = 75%, CPU média = 55%, memória máxima = 7,0 GB	1000 por minuto
500 RDS, 10.000 sessões	Interrupção	3 minutos	CPU máxima = 15%, CPU média =	10 minutos	CPU máxima = 45%, CPU média =	1000 por minuto

CARGAS DE TRABALHO DE TESTE	CONDIÇÃO DO SITE	TEMPO DE REGISTRO DO VDA	USO DE CPU E MEMÓRIA DE REGISTRO	DURAÇÃO DO TESTE DE INICIALIZAÇÃO	USO DE CPU E MEMÓRIA NA INICIALIZAÇÃO DA SESSÃO	TAXA DE INICIALIZAÇÃO
			5%, memória máxima = 7,5		40%, memória máxima = 7,5 GB	

Cargas de trabalho máximas

Essas cargas de trabalho foram testadas com 8 vCPUs e 10 GB de memória.

CARGAS DE TRABALHO DE TESTE	CONDIÇÃO DO SITE	TEMPO DE REGISTRO DO VDA	USO DE CPU E MEMÓRIA NO REGISTRO	DURAÇÃO DO TESTE DE INICIALIZAÇÃO	USO DE CPU E MEMÓRIA NA INICIALIZAÇÃO DA SESSÃO	TAXA DE INICIALIZAÇÃO
10.000 VDIs	Online	3–4 minutos	CPU máxima = 85%, CPU média = 10%, memória máxima = 8,5 GB	7 minutos	CPU máxima = 66%, CPU média = 28%, memória máxima = 7,0 GB	1400 por minuto
10.000 VDIs	Interrupção	4–5 minutos	CPU máxima = 90%, CPU média = 17%, memória máxima = 8,2 GB	5 minutos	CPU máxima = 90%, CPU média = 45%, memória máxima = 8,5 GB	2000 por minuto

CARGAS DE TRABALHO DE TESTE	CONDIÇÃO DO SITE	TEMPO DE REGISTRO DO VDA	USO DE CPU E MEMÓRIA NO REGISTRO	DURAÇÃO DO TESTE DE INICIALIZAÇÃO	USO DE CPU E MEMÓRIA NA INICIALIZAÇÃO DA SESSÃO	TAXA DE INICIALIZAÇÃO
1000 RDS, 20.000 sessões	Online	1–2 minutos	CPU máxima = 60%, CPU média = 20%, memória máxima = 8,6 GB	17 minutos	CPU máxima = 66%, CPU média = 25%, memória máxima = 6,8 GB	1200 por minuto
1000 RDS, 20.000 sessões	Interrupção	3–4 minutos	CPU máxima = 22%, CPU média = 10%, memória máxima = 8,5	21 minutos	CPU máxima = 90%, CPU média = 50%, memória máxima = 7,5 GB	1000 por minuto

Nota:

As cargas de trabalho mostradas aqui são as cargas de trabalho máximas recomendadas para um local de recurso. Para suportar cargas de trabalho maiores, adicione mais locais de recurso.

Usos de recursos de sincronização de configuração

O processo de sincronização de configuração mantém os Cloud Connectors atualizados com o Citrix DaaS. As atualizações são enviadas automaticamente para os Cloud Connectors para garantir que os Cloud Connectors estejam prontos para assumir o gerenciamento se ocorrer uma interrupção. A sincronização de configuração atualiza o banco de dados LHC, SQL Express Server LocalDB. O processo importa os dados para um banco de dados temporário e, em seguida, muda

para esse banco de dados após a importação. Isso garante que sempre haja um banco de dados LHC pronto para assumir.

O uso da CPU, memória e disco é temporariamente aumentado enquanto os dados são importados para o banco de dados temporário.

Condições de teste:

- Testado em um AMD EPYC de 8 vCPU
- O banco de dados de configuração do site importado era para um ambiente com um total de 80.000 VDAs e 300.000 usuários em todo o site (três turnos de 100.000 usuários)
- O tempo de importação de dados foi testado em um local de recurso com 10.000 VDI

Resultados do teste:

- **Tempo de importação de dados:** 7–10 minutos
- **Uso da CPU:**
  - máximo = 25%
  - média = 15%
- **Uso da memória:**
  - aumento de aproximadamente 2 GB a 3 GB
- **Uso do disco:**
  - pico de leitura de disco de 4 MB/s
  - pico de gravação de disco de 18 MB/s
  - pico de gravação de disco de 70 MB/s durante o download e a gravação de arquivos de configuração xml
  - pico de leitura de disco de 4 MB/s na conclusão da importação
- **Tamanho do banco de dados LHC:**
  - arquivo de banco de dados de 400–500 MB
  - banco de dados de log de 200–300 MB

Considerações adicionais sobre o uso de recursos:

- Durante a importação, os dados completos de configuração do site são baixados. Esse download pode causar um pico de memória, dependendo do tamanho do site. Se picos de

memória estiverem ocorrendo durante as sincronizações de configuração, considere aumentar o tamanho dos Cloud Connectors.

- O site testado usou aproximadamente 800 MB para o banco de dados e arquivos de log do banco de dados combinados. Durante uma sincronização de configuração, esses arquivos são duplicados com um tamanho combinado máximo de aproximadamente 1600 MB. Certifique-se de que seu Cloud Connector tenha espaço em disco suficiente para os arquivos duplicados. O processo de sincronização de configuração falha se o disco estiver cheio.

Instalar VDAs

Introdução

Este artigo começa com uma descrição dos VDAs do Windows e dos instaladores de VDA disponíveis. O restante do artigo descreve as etapas do assistente de instalação do VDA. Equivalentes de linha de comando são fornecidos. Para obter detalhes, consulte Instalar VDAs usando a linha de comando.

Para obter informações sobre VDAs Linux, consulte Linux Virtual Delivery Agent.

Assista a uma introdução aos VDAs.



Considerações sobre a instalação

O artigo Citrix DaaS descreve o que são os VDAs e o que eles fazem. Aqui estão mais informações.

- **Coleta de análises:** As análises são coletadas automaticamente quando você instala ou atualiza componentes. Por padrão, esses dados são carregados para a Citrix automaticamente quando a instalação é concluída. Além disso, ao instalar componentes, você é automaticamente inscrito no Programa de Melhoria da Experiência do Cliente Citrix (CEIP), que carrega dados anônimos. Além disso, durante uma instalação ou atualização, é oferecida a oportunidade de se inscrever no Call Home.

  Se uma instalação de VDA falhar, um analisador MSI analisa o log MSI com falha, exibindo o código de erro exato. O analisador sugere um artigo CTX, se for um problema conhecido. O analisador também coleta dados anonimizados sobre o código de erro da falha. Esses dados são incluídos com outros dados coletados pelo CEIP. Se você encerrar a inscrição no CEIP, os dados coletados pelo analisador MSI não serão mais enviados à Citrix.

Para obter informações sobre esses programas, consulte Citrix Insight Services.

- **Aplicativo Citrix Workspace™:** O aplicativo Citrix Workspace para Windows não é instalado por padrão ao instalar um VDA. Você pode baixar e instalar ou atualizar o aplicativo Citrix Workspace para Windows e outros aplicativos Citrix Workspace no site da Citrix. Alternativamente, você pode disponibilizar esses aplicativos Citrix Workspace a partir do Workspace ou de um servidor StoreFront™.
- **Serviço Spooler de Impressão:** O Serviço Spooler de Impressão da Microsoft deve estar habilitado. Você não pode instalar um VDA com sucesso se esse serviço estiver desabilitado.
- **Microsoft Media Foundation:** A maioria das edições do Windows suportadas já vem com o Media Foundation instalado. Se a máquina na qual você está instalando um VDA não tiver o Microsoft Media Foundation (como as edições N), vários recursos multimídia não serão instalados e não funcionarão.
  - Redirecionamento de Flash
  - Redirecionamento de Mídia do Windows
  - Redirecionamento de Vídeo HTML5
  - Redirecionamento de Webcam HDX™ RealTime

  Você pode reconhecer a limitação ou encerrar a instalação do VDA e reiniciá-la mais tarde, após instalar o Media Foundation. Na interface gráfica, essa escolha é apresentada em uma mensagem. Na linha de comando, você pode usar a opção `/no_mediafoundation_ack` para reconhecer a limitação.
- **Grupo de usuários local:** Ao instalar o VDA, um novo grupo de usuários local chamado Direct Access Users é criado automaticamente. Para um VDA de SO de sessão única, esse grupo se aplica apenas a conexões RDP. Para um VDA de SO de várias sessões, esse grupo se aplica a conexões ICA® e RDP.
- **Requisito de endereço do Cloud Connector:** O VDA deve ter pelo menos um endereço de Cloud Connector válido (no mesmo local de recurso) com o qual se comunicar. Caso contrário, as sessões não poderão ser estabelecidas. Você especifica os endereços do Cloud Connector ao instalar o VDA. Para obter informações sobre outras maneiras de especificar endereços do Cloud Connector onde os VDAs podem se registrar, consulte Registro de VDA.
- **Considerações sobre o sistema operacional:**
  - Revise os Requisitos do sistema para plataformas, sistemas operacionais e versões suportados.
  - Certifique-se de que cada sistema operacional mantenha as atualizações mais recentes.

    - Certifique-se de que os VDAs tenham relógios de sistema sincronizados. A infraestrutura Kerberos que protege a comunicação entre as máquinas requer sincronização.
    - Orientações de otimização para máquinas Windows 10 estão disponíveis em CTX216252.
    - Se você tentar instalar (ou atualizar para) um VDA Windows em um SO que não é compatível com essa versão do VDA, uma mensagem descreverá suas opções. Para obter mais informações, consulte Requisitos do sistema e Sistemas operacionais anteriores.

- **MSIs instalados:** Vários MSIs são instalados automaticamente quando você instala um VDA. Você pode impedir a instalação de alguns MSIs na página **Componentes Adicionais** da interface gráfica ou com a opção `/exclude` na CLI. Para outros, a única maneira de impedir a instalação é com a opção CLI `/exclude`.
- **Ingressado no domínio:** Certifique-se de que a máquina esteja ingressada no domínio antes de instalar o software VDA.

Reinicializações durante a instalação do VDA

É necessário reiniciar ao final da instalação do VDA. Essa reinicialização ocorre automaticamente por padrão.

Para minimizar o número de outras reinicializações necessárias durante a instalação do VDA:

- Certifique-se de que uma versão compatível do Microsoft .NET Framework esteja instalada antes de iniciar a instalação do VDA.
- Para máquinas com SO Windows multi-sessão, instale e habilite os serviços de função RDS antes de instalar o VDA.

Se você não instalar esses pré-requisitos antes de instalar o VDA:

- Se você estiver usando a interface gráfica ou a interface de linha de comando sem a opção `/noreboot`, a máquina reinicia automaticamente após a instalação do pré-requisito.
- Se você estiver usando a interface de linha de comando com a opção `/noreboot`, você deve iniciar a reinicialização.

Após cada reinicialização, a instalação do VDA continua. Se você estiver instalando pela linha de comando, pode impedir a retomada automática com a opção `/noresume`.

Ao atualizar um VDA para a versão 7.17 ou uma versão posterior compatível, uma reinicialização ocorre durante a atualização. Essa reinicialização não pode ser evitada.

Restaurar em caso de falha na instalação ou atualização

> **Nota:**
>
> Este recurso está disponível apenas para VDAs de sessão única.

> Se uma instalação ou atualização de VDA de sessão única falhar, e o recurso "restaurar em caso de falha" estiver habilitado, a máquina é retornada a um ponto de restauração que foi definido antes do início da instalação ou atualização.

Quando uma instalação ou atualização de VDA de sessão única é iniciada com este recurso habilitado, o instalador cria um ponto de restauração do sistema antes de iniciar a instalação ou atualização real. Se a instalação ou atualização do VDA falhar, a máquina é retornada ao estado do ponto de restauração. A pasta `%temp%/Citrix` contém logs de implantação e outras informações sobre a restauração.

Por padrão, este recurso está desabilitado.

Se você planeja habilitar este recurso, certifique-se de que a restauração do sistema não esteja desabilitada por meio de uma configuração de GPO (`Computer Configuration > Administrative Templates > System > System Restore`).

Para habilitar este recurso ao instalar ou atualizar um VDA de sessão única:

- Ao usar a interface gráfica de um instalador VDA (como usando **Autostart** ou o comando `XenDesktopVDASetup.exe` sem quaisquer opções de restauração ou silenciosas), selecione a caixa de seleção **Habilitar restauração automática se a atualização falhar** na página **Resumo**.

  Se a instalação/atualização for concluída com êxito, o ponto de restauração não será usado, mas será retido.

- Execute um instalador VDA com a opção `/enablerestore` ou `/enablerestorecleanup`.
  - Se você usar a opção `/enablerestorecleanup`, e a instalação/atualização for concluída com êxito, o ponto de restauração será removido automaticamente.
  - Se você usar a opção `/enablerestore`, e a instalação/atualização for concluída com êxito, o ponto de restauração não será usado, mas será retido.

Instaladores VDA

Os instaladores VDA podem ser baixados diretamente do console Citrix Cloud™.

Por padrão, os arquivos nos instaladores autoextraíveis são extraídos para a pasta `Temp`. Os arquivos extraídos para a pasta `Temp` são automaticamente excluídos após a conclusão da instalação. Alternativamente, você pode usar o comando `/extract` com um caminho absoluto.

Três instaladores VDA autônomos estão disponíveis para download.

VDAServerSetup.exe Instala um VDA de SO multi-sessão.

VDAWorkstationSetup.exe Instala um VDA de SO de sessão única.

VDAWorkstationCoreSetup.exe Instala um VDA de SO de sessão única otimizado para implantações de Acesso Remoto a PC ou instalações VDI principais. O Acesso Remoto a PC usa máquinas físicas. As instalações VDI principais são VMs que não estão sendo usadas como uma imagem. Este instalador implanta apenas os serviços essenciais necessários para conexões VDA. Portanto, ele suporta apenas um subconjunto das opções válidas com o instalador VDAWorkstationSetup.

Para obter mais informações, consulte Instalar VDA para suas respectivas versões.

Solução de problemas

No display do Studio para um grupo de entrega, a entrada **Versão do VDA Instalado** no painel Detalhes pode não ser a versão instalada nas máquinas. O display de Programas e Recursos do Windows da máquina mostra a versão real do VDA.

Citrix Optimizer

O Citrix Optimizer é uma ferramenta para o sistema operacional Windows que ajuda os administradores Citrix a otimizar VDAs removendo e otimizando vários componentes.

Após instalar um VDA e concluir a reinicialização final, baixe e instale o Citrix Optimizer. Consulte CTX224676. O artigo CTX contém o pacote de download, além de instruções sobre como instalar e usar o Citrix Optimizer.

Personalizar um VDA

Posteriormente, para personalizar (alterar informações de) um VDA instalado:

1. No recurso do Windows para remover ou alterar programas, selecione **Citrix Virtual Delivery Agent** ou **Citrix Remote PC Access/VDI Core Services VDA**. Em seguida, clique com o botão direito e selecione **Alterar**.
2. Selecione **Personalizar Configurações do Virtual Delivery Agent**.

Quando o instalador for iniciado, altere as configurações disponíveis.

Personalizar a porta para comunicação com os Cloud Connectors

Você pode personalizar a porta que os VDAs usam para se comunicar com os Cloud Connectors com base em seus requisitos de segurança específicos. Esse recurso é útil se sua equipe de segurança não permite que a porta padrão (porta 80) esteja aberta ou se a porta padrão já estiver em uso.

> **Nota:**

> Ao alterar o número da porta padrão, apenas valores dentro do intervalo de 1024 a 65535 são suportados.

> Para personalizar a porta, conclua as seguintes etapas:

1. Adicionar o número da porta VDA nos Citrix Cloud Connectors
2. Configuração adicional do Citrix Cloud Connector™ ao usar o Rendezvous V1
3. Adicionar o número da porta VDA nos VDAs

Adicionar o número da porta VDA nos Citrix Cloud Connectors

Vá para o Citrix Cloud Connector e execute os dois comandos PowerShell a seguir:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe' -VdaPort <port number>`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe' -VdaPort <port number> -ConfigureFirewall`

Exemplo:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe' -VdaPort 18000`

- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe' -VdaPort 18000 -ConfigureFirewall`

Ao personalizar a porta, considere o seguinte:

- Você deve usar o mesmo número de porta em ambos os comandos.
- Você deve executar ambos os comandos *em todos os Cloud Connectors*.
- Para se comunicar com sucesso com os Cloud Connectors, certifique-se de que todos os VDAs usem o mesmo número de porta.
- A porta que você configura persiste nas atualizações do conector.

Configuração adicional do Citrix Cloud Connector ao usar o Rendezvous V1

Defina a seguinte chave de registro em cada Citrix Cloud Connector:

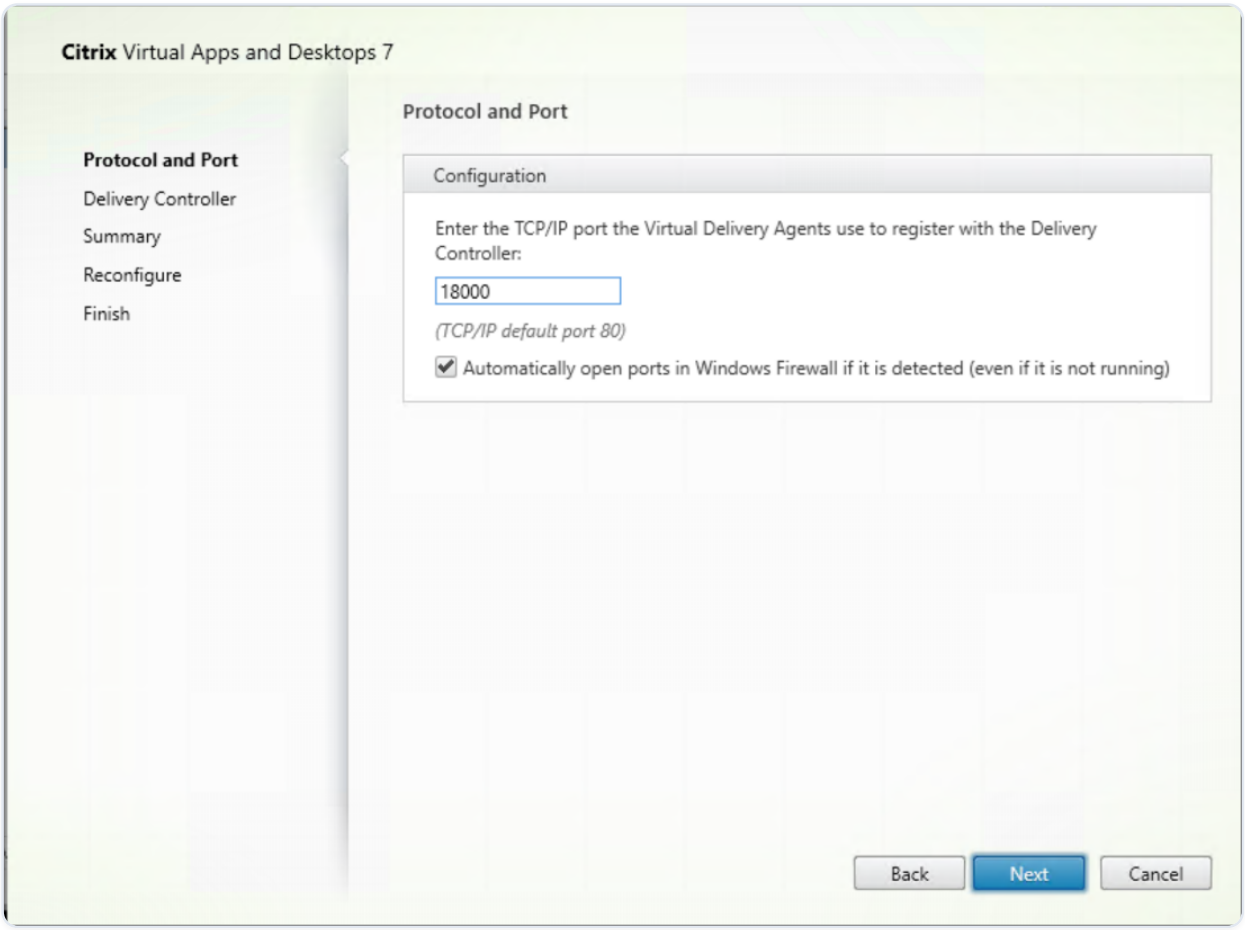
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist`

Nome: `WorkerPortNumber` Tipo: `REG_DWORD` Valor: `<port number>`

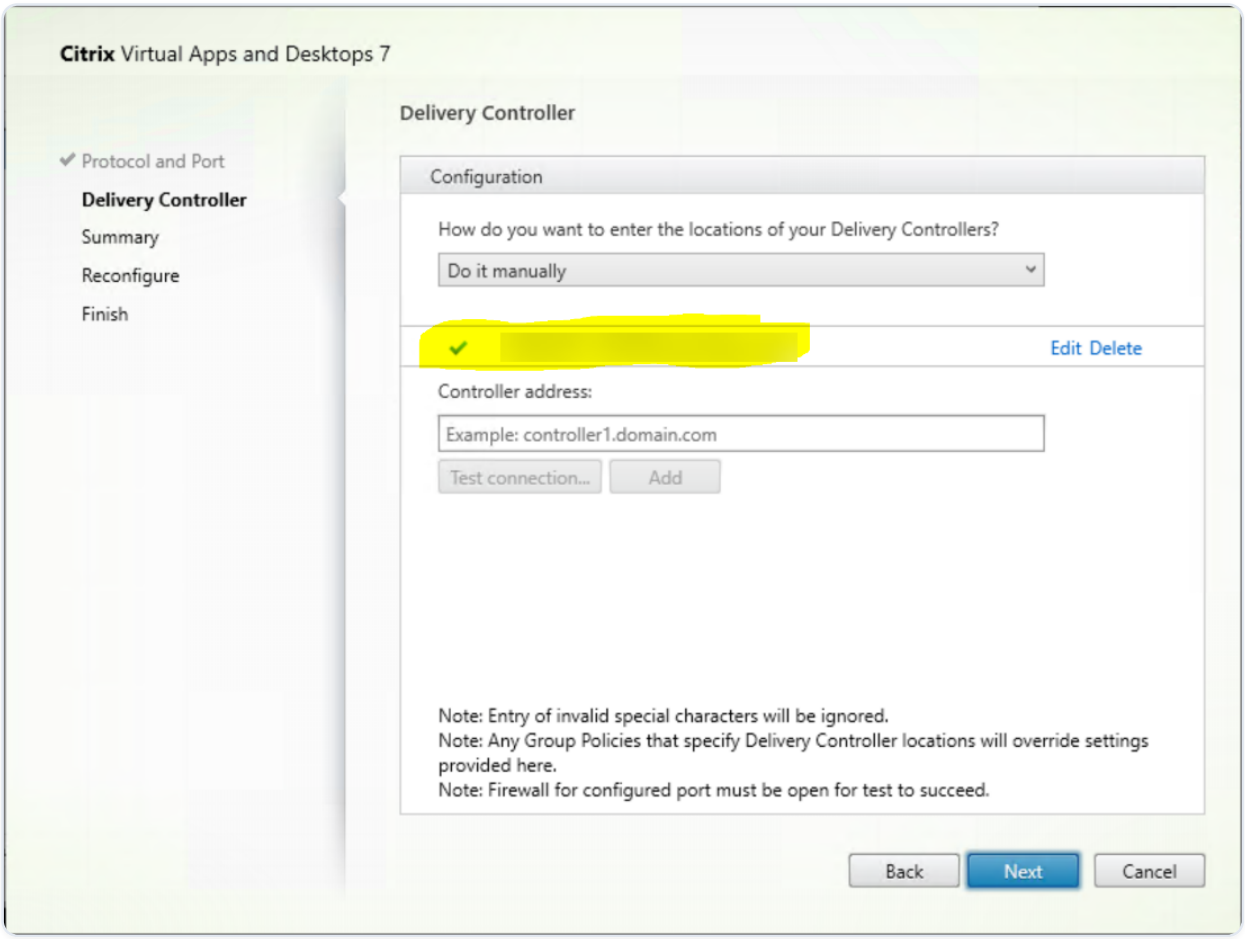
Adicionar o número da porta VDA nos VDAs

Instale o VDA com as configurações padrão e configure-o da seguinte forma. Se o VDA já estiver instalado, continue com as etapas abaixo.

1. No VDA, abra **XenDesktopVdaSetup.exe**, que está localizado em `C:\Program Files\Citrix\XenDesktopVdaSetup\XenDesktopVdaSetup.exe`.
2. Na página **Protocol and Port**, adicione o número da porta personalizada.



3. Na página **Delivery Controller™**, insira o FQDN do Controller.



4. Clique em **Next** para prosseguir com o assistente e concluir a configuração.

Os números das portas são então reconfigurados com sucesso.

> **Nota:**

> Você pode ver a seguinte mensagem de erro ao testar uma conexão do Controller: Nenhuma instância em execução de um Controller encontrada em < o endereço do Controller que você inseriu >. Se o endereço estiver correto, você pode ignorar a mensagem.

Solução de problemas

Para verificar se as portas personalizadas estão configuradas corretamente, vá para o Cloud Connector e execute as seguintes etapas de solução de problemas:

1. Verifique se as duas chaves de registro a seguir existem.

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist Nome: CustomVDAPortNumber Tipo: REG_DWORD Dados: 18000

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist Nome: CustomVDAPortNumberHA Tipo: REG_DWORD Dados: 18000

2. Execute o seguinte comando para criar um arquivo .txt.

   - `netsh http show urlacl > <filepath>.txt`

   Exemplo:

   - `netsh http show urlacl > c:\reservations.txt`

3. Abra o arquivo .txt e verifique as quatro URLs a seguir para confirmar se a porta correta está sendo usada.

   - `http://+:18000/Citrix/CdsController/IRegistrar/`
   - `http://+:18000/Citrix/CdsController/ITicketing/`
   - `http://+:18000/Citrix/CdsController/IDynamicDataSink/`
   - `http://+:18000/Citrix/CdsController/INotifyBroker/`

4. Verifique se as duas regras de firewall a seguir foram criadas e se as portas necessárias estão abertas.

   - Citrix XaXdProxy
   - Citrix Broker Service (TCP-In)

Outras informações

- Depois de instalar um VDA, você pode verificar a integridade e a disponibilidade do site e seus componentes com uma verificação de integridade da nuvem.

Próximos passos

Criar catálogos de máquinas.

Para revisar todo o processo de configuração, consulte Planejar e construir uma implantação.

Instalar VDAs usando a linha de comando

Introdução

Este artigo se aplica à instalação, atualização e personalização de Virtual Delivery Agents (VDAs) em máquinas com sistemas operacionais Windows.

Este artigo descreve como emitir comandos de instalação do VDA. Antes de iniciar uma instalação, revise Instalar VDAs para saber mais sobre considerações de instalação, instaladores e o que você especifica durante a instalação.

Instalar um VDA a partir da linha de comando

Para instalar um VDA (e ver o progresso da execução do comando e os valores de retorno), você deve ter permissões administrativas elevadas ou usar **Executar como administrador**.

1. Na máquina onde você está instalando o VDA, faça login em Citrix Cloud.
2. No menu superior esquerdo, selecione **Soluções > DaaS**.
3. No lado superior direito, clique em **Downloads** e selecione **Download VDA**. Você será redirecionado para a página de download do VDA. Encontre o instalador do VDA que deseja e clique em **Download File**.
4. Após a conclusão do download, execute seu nome. Use as opções descritas neste artigo.
    - Para o Virtual Delivery Agent de SO multi-sessão, execute `VDAServerSetup.exe`
    - Para o Virtual Delivery Agent de SO de sessão única, execute `VDAWorkstationSetup.exe`
    - Para o Virtual Delivery Agent de Serviços Principais de SO de sessão única, execute `VDAWorkstationCoreSetup.exe`

Para extrair os arquivos antes de instalá-los, use `/extract` com o caminho absoluto, por exemplo `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. (O diretório deve existir. Caso contrário, a extração falhará.) Em seguida, em um comando separado, execute o comando apropriado, usando as opções válidas listadas neste artigo.

- Para `VDAServerSetup_XXXX.exe`, execute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
- Para `VDAWorkstationCoreSetup_XXXX.exe`, execute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
- Para `VDAWorkstationSetup_XXXX.exe`, execute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

Opções de linha de comando para instalar um VDA

As seguintes opções são válidas com um ou mais dos comandos: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` e `VDAWorkstationCoreSetup.exe`.

- **/components** *componente*\[,*componente*\]

  Lista de componentes separados por vírgula para instalar ou remover. Os valores válidos são:

  - **VDA:** Virtual Delivery Agent
  - **PLUGINS:** aplicativo Citrix Workspace™ para Windows

  Para instalar o VDA e o aplicativo Citrix Workspace, especifique `/components vda,plugins`.

  Se a opção `plugins` for omitida, somente o VDA é instalado (e não o aplicativo Citrix Workspace).

  Esta opção não é válida ao usar o instalador `VDAWorkstationCoreSetup.exe`. Esse instalador não pode instalar o aplicativo Citrix Workspace.

- **/controllers** "*controlador ...*"

  FQDNs de Citrix Cloud Connectors separados por espaço com os quais o VDA pode se comunicar, entre aspas retas. Não especifique as opções `/site_guid` e `/controllers` simultaneamente.

- **/desabilitarmétricasdeexperiência**

  Impede o upload automático de análises coletadas durante a instalação, atualização ou remoção para a Citrix.

- **/enable_hdx_ports**

  Abre as portas no firewall do Windows exigidas pelo VDA e pelos recursos habilitados (exceto Assistência Remota do Windows), se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja habilitado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente. Para obter informações sobre portas, consulte Portas de rede.

  Para abrir as portas UDP para o transporte adaptável HDX, especifique a opção `/enable_hdx_udp_ports`, além da opção `/enable_hdx_ports`.

- **/enable_hdx_udp_ports**

  Abre as portas UDP no firewall do Windows que o transporte adaptável HDX exige, se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja habilitado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente. Para obter informações sobre portas, consulte Portas de rede.

Para abrir as portas que o VDA usa, especifique a opção `/enable_hdx_ports`, além da opção `/enable_hdx_udp_ports`.

- **/enable_real_time_transport**

  Habilita ou desabilita o uso de UDP para pacotes de áudio (Transporte de Áudio em Tempo Real para áudio). Habilitar esse recurso pode melhorar o desempenho do áudio. Inclua a opção `/enable_hdx_ports` se você quiser que as portas UDP sejam abertas automaticamente quando o Serviço de Firewall do Windows for detectado.

- **/enable_remote_assistance**

  Habilita o recurso de sombreamento na Assistência Remota do Windows para uso com as funções de **Monitoramento**. Se você especificar esta opção, a Assistência Remota do Windows abrirá as portas dinâmicas no firewall.

- **/enablerestore** ou **/enablerestorecleanup**

  (Válido apenas para VDAs de sessão única) Habilita o retorno automático ao ponto de restauração, se a instalação ou atualização do VDA falhar.

  Se a instalação/atualização for concluída com êxito:

  - `/enablerestorecleanup` instrui o instalador a remover o ponto de restauração.
  - `/enablerestore` instrui o instalador a manter o ponto de restauração, mesmo que não tenha sido usado.

  Para obter detalhes, consulte Restaurar em caso de falha na instalação ou atualização.

- **/enable_ss_ports**

  Abre as portas no Firewall do Windows que são necessárias para o compartilhamento de tela, se o Serviço de Firewall do Windows for detectado, mesmo que o firewall não esteja ativado. Se você estiver usando um firewall diferente ou nenhum firewall, deverá configurar o firewall manualmente.

- **/exclude** "*componente*"\[,"*componente*"\]

  Impede a instalação de um ou mais componentes opcionais separados por vírgulas, cada um entre aspas retas. Por exemplo, a instalação ou atualização de um VDA em uma imagem gerenciada por MCS requer o componente Serviço de Identidade da Máquina. Os valores válidos são:

  - Serviço de Identidade da Máquina

- Citrix Profile Management
- Citrix Profile Management WMI Plug-in
- Personalização Citrix para App-V - VDA
- Citrix MCS IODriver
- Citrix VDA Upgrade Agent
- Citrix Rendezvous V2

Excluir o Citrix Profile Management da instalação (`/exclude "Citrix Profile Management"`) afeta o monitoramento e a solução de problemas de VDAs a partir do console **Monitor**. Nas páginas **Detalhes do usuário** e **Ponto de extremidade**, o painel Personalização e o painel Duração do Logon falham. Nas páginas **Painel** e **Tendências**, o painel Duração Média do Logon exibe dados apenas para máquinas que têm o Profile Management instalado.

Mesmo que você esteja usando uma solução de Profile Management de terceiros, a Citrix recomenda que você instale e execute o Serviço Citrix Profile Management. A ativação do Serviço Citrix Profile Management não é obrigatória.

Se você planeja usar o MCS para provisionar VMs, não exclua o Serviço de Identidade da Máquina.

Se você especificar `/exclude` e `/includeadditional` com o mesmo nome de componente, o componente não será instalado.

Esta opção não é válida ao usar o instalador `VDAWorkstationCoreSetup.exe`. Esse instalador exclui automaticamente muitos desses itens.

- **/h** ou **/help**

  Exibe a ajuda do comando.

- **/includeadditional** "*componente*"\[,"*componente*"\] ...

  Inclui a instalação de um ou mais componentes opcionais separados por vírgulas, cada um entre aspas simples. Os nomes dos componentes diferenciam maiúsculas de minúsculas.

  Esta opção pode ser útil ao criar uma implantação de Acesso Remoto a PC e desejar instalar componentes que não são incluídos por padrão. Os valores válidos são:

  - Citrix Profile Management
  - Citrix Profile Management WMI Plug-in

- Citrix Personalização para App-V - VDA
- Citrix MCS IODriver
- Citrix VDA Upgrade Agent
- Citrix Rendezvous V2
- Camada de personalização do usuário
- Citrix Web Socket VDA Registration Tool

Se você especificar `/exclude` e `/includeadditional` com o mesmo nome de componente, esse componente não será instalado.

- **/installdir** *diretório*

  Diretório vazio existente onde os componentes serão instalados. Padrão = c:\Program Files\Citrix.

- **/install_mcsio_driver**

  Não use. Em vez disso, use `/includeadditional "Citrix MCS IODriver"` ou `/exclude "Citrix MCS IODriver"`

- **/logpath** *caminho*

  Local do arquivo de log. A pasta especificada deve existir. O instalador não a cria. Padrão = "%TEMP%\Citrix\XenDesktop Installer"

  Esta opção não está disponível na interface gráfica.

- **/imagem mestre**

  Válido apenas ao instalar um VDA em uma VM. Configura o VDA como uma imagem. Esta opção é equivalente a `/mastermcsimage`.

  Esta opção não é válida ao usar o instalador `VDAWorkstationCoreSetup.exe`.

- **/imagem mestre mcs**

  Especifica que esta máquina será usada como uma imagem com o Machine Creation Services. Esta opção é equivalente a `/masterimage`.

- **/imagem mestre pvs**

  Especifica que esta máquina será usada como uma imagem com o Citrix Provisioning™ ou uma ferramenta de provisionamento de terceiros (como o Microsoft System Center Configuration Manager).

- **/no_mediafoundation_ack**

  Reconhece que o Microsoft Media Foundation não está instalado e que vários recursos multimídia HDX™ não estão instalados e não funcionam. Se esta opção for omitida e o Media Foundation não estiver instalado, a instalação do VDA falhará. A maioria das edições do Windows suportadas já vem com o Media Foundation instalado, exceto as edições N.

- **/semexperiênciadedesktop**

  Válido apenas ao instalar um VDA de SO multi-sessão. Impede a habilitação do recurso Experiência de Área de Trabalho Aprimorada. Este recurso também é controlado pela configuração de política Citrix de Experiência de Área de Trabalho Aprimorada.

- **/semreinicialização**

  Impede uma reinicialização após a instalação. O VDA não pode ser usado antes de uma reinicialização.

- **/semretomar**

  Por padrão, quando uma reinicialização da máquina é necessária durante uma instalação, o instalador é retomado automaticamente após a conclusão da reinicialização. Para substituir o padrão, especifique `/noresume`. Isso pode ser útil se você precisar remontar a mídia ou quiser capturar informações durante uma instalação automatizada.

- **/númerodaporta** *porta*

  Válido apenas quando a opção `/reconfig` é especificada. Número da porta a ser habilitada para comunicações entre o VDA e o Controller. A porta configurada anteriormente é desabilitada, a menos que seja a porta 80.

- **/configuraçãodoproxy** "*endereço ou caminho do arquivo PAC*"

  Válido apenas se o comando contiver `/includeadditional "Citrix Rendezvous V2"`. O endereço ou caminho do arquivo PAC do proxy para uso com o protocolo Rendezvous. Para detalhes do recurso, consulte protocolo Rendezvous.

  - Formato do endereço do proxy: `http://<url-or-ip>:<port>`
  - Formato do arquivo PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** ou **/passive**

  Nenhuma interface de usuário aparece durante a instalação. A única evidência do processo de instalação e configuração está no Gerenciador de Tarefas do Windows. Se esta opção for omitida, a interface gráfica será iniciada.

- **/reconfigurar**

  Personaliza as configurações do VDA configuradas anteriormente quando usado com as opções `/portnumber`, `/controllers` ou `/enable_hdx_ports`. Se você especificar esta opção sem também especificar a opção `/quiet`, a interface gráfica para personalizar o VDA será iniciada.

- **/pcremoto**

  Válido apenas para implantações de Acesso Remoto a PC (SO de sessão única) ou conexões intermediadas (SO de múltiplas sessões).

  Esta opção não é válida ao usar o instalador `VDAWorkstationCoreSetup.exe`. Esse instalador exclui automaticamente a instalação desses componentes.

- **/remove_appdisk_ack**

  Autoriza o instalador do VDA a desinstalar o plug-in AppDisks™ VDA, se estiver instalado.

- **/remove_pvd_ack**

  Autoriza o instalador do VDA a desinstalar o Personal vDisk, se estiver instalado.

- **/remover**

  Remove os componentes especificados com a opção `/components`.

- **/removertudo**

  Remove o VDA. Não remove o aplicativo Citrix Workspace (se instalado).

- **/enviarmetricasdeexperiencia**

  Envia automaticamente análises coletadas durante a instalação, atualização ou remoção para a Citrix. Se esta opção for omitida (ou a opção `/disableexperiencemetrics` for especificada), as análises são coletadas localmente, mas não são enviadas automaticamente.

- **servidorvdi**

  Instala um VDA de SO de sessão única em um servidor Windows compatível. Omita esta opção ao instalar um VDA de várias sessões em um servidor Windows. Antes de usar esta opção, consulte Server VDI.

- **local_guid** *guid*

  Identificador Globalmente Único da Unidade Organizacional (OU) do Active Directory do site. Isso associa uma área de trabalho virtual a um site quando você está usando o Active

Directory para descoberta (a atualização automática é o método de descoberta recomendado e padrão). O GUID do site é uma propriedade do site exibida no Studio. Não especifique as opções `/site_guid` e `/controllers`.

- **dirtemp** *diretório*

  Diretório para armazenar arquivos temporários durante a instalação. Padrão = c:\Windows\Temp.

  Esta opção não está disponível na interface gráfica.

- **máquinavirtual**

  Válido apenas ao instalar um VDA em uma VM. Substitui a detecção pelo instalador de uma máquina física, onde as informações do BIOS passadas para as VMs as fazem parecer máquinas físicas.

  Esta opção não está disponível na interface gráfica.

- **xendesktopnuvem**

  Indica que o VDA está instalado em uma implantação do Citrix DaaS (Citrix Cloud™).

Exemplos: Instalar um VDA

- **Instalar um VDA em um SO de várias sessões.** O comando a seguir instala um VDA em um SO de várias sessões.

  ```
  VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com" /
  enable_hdx_ports /masterimage
  ```

  O VDA será usado como uma imagem.

- **Instalar um VDA de SO multi-sessão ou VDA de SO de sessão única.** O comando a seguir instala um VDA de SO multi-sessão ou um VDA de SO de sessão única.

  ```
  VDAServerSetup_XXXX.exe /quiet /controllers "ddc1.abc.com","ddc2.abc.com" /
  enable_hdx_ports /enable_Remote_Assistance /enable_real_time_transport /
  enable_ss_ports /noreboot
  ```

  Separe cada FQDN do delivery controller™ por uma vírgula. Observe que `XXXX` representa a versão do VDA.

- **Instalar um VDA de Serviços Essenciais em um SO de sessão única.** O comando a seguir instala um VDA de Serviços Essenciais em um SO de sessão única para uso em um acesso remoto de PC ou implantação de VDA.

`VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.domain.com" /enable_hdx_ports /noreboot`

O aplicativo Citrix Workspace e outros serviços não essenciais não são instalados. O endereço de um Cloud Connector é especificado, e as portas no Serviço de Firewall do Windows são abertas automaticamente. O administrador lida com as reinicializações.

Personalizar um VDA usando a linha de comando

Depois de instalar um VDA, você pode personalizar várias configurações. Execute `XenDesktopVDASetup.exe`, usando uma ou mais das seguintes opções.

- `/reconfigure` (obrigatório ao personalizar um VDA)
- `/h` ou `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Onde ir em seguida

- Criar catálogos de máquinas
- Para revisar todo o processo de configuração, consulte Planejar e construir uma implantação.

Comunicação WebSocket entre VDA e Delivery Controller™

Este artigo descreve como configurar uma conexão WebSocket para comunicação entre VDAs e Delivery Controllers como uma alternativa ao uso da comunicação WCF. Oferece o benefício de que apenas a porta TLS 443 é usada para a comunicação do VDA para o Delivery Controller.

Atualmente, isso está disponível apenas para máquinas provisionadas por MCS.

Como funciona

A seção a seguir descreve o fluxo de trabalho para a conexão WebSocket entre um Delivery Controller e um VDA:

1. Os administradores iniciam o processo provisionando VDAs usando o Machine Creation Service (MCS).

2. Durante o processo de provisionamento do MCS, o MCS gera pares de chaves pública-privada para cada VDA e registra as chaves públicas com o serviço de confiança FMA no Delivery Controller. O MCS salva o par de chaves pública-privada como um arquivo no disco de identidade nos VDAs.
3. Quando a máquina VDA inicializa, o agente MCS instalado na máquina VDA lê o par de chaves do disco de identidade e grava essas informações no local do registro do VDA.
4. O agente broker instalado no VDA lê os pares de chaves do registro e gera uma solicitação WebSocket habilitada para SSL para o Delivery Controller com um cabeçalho de autenticação de chave de serviço assinado pela chave privada.
5. O Delivery Controller verifica o cabeçalho de autenticação de chave de serviço assinado com a chave pública do serviço de confiança FMA.
6. Assim que a verificação é concluída, o sistema estabelece a conexão WebSocket entre o VDA e o Delivery Controller.

Suporte a WebSocket

Procedimento

Siga as instruções para configurar uma conexão WebSocket:

1. Crie um catálogo de máquinas para VDAs unidos ao AD com provisionamento MCS. Para obter mais informações, consulte Criar catálogo de máquinas.
2. Crie um grupo de entrega e adicione seu VDA a ele. Para obter mais informações, consulte Criar grupos de entrega.
3. Habilite uma conexão WebSocket no VDA. Execute o seguinte comando PowerShell no VDA:

   ```
   New-ItemProperty
   "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent
   \WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
   ```

   - Para verificar se o WebSocket está habilitado, verifique o seguinte valor da chave de registro. O valor de `Enabled` deve ser 1.

     Chave:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAge
     nt\WebSocket
     ```

Nome: Enabled

Tipo: REG_DWORD

Valor: 1

Criar e gerenciar conexões

Introdução

Configurar uma conexão envolve selecionar o tipo de conexão na lista de hipervisores e serviços de nuvem suportados, e escolher os recursos de armazenamento e rede apropriados para essa conexão.

> **Nota:**
>
> Você deve ter privilégios de Administrador Completo para executar tarefas relacionadas ao gerenciamento de conexões e recursos.

Onde encontrar informações sobre tipos de conexão

Requisitos do sistema fornecem uma lista de hipervisores e versões de serviços de nuvem suportados, juntamente com links para artigos para cada host específico.

Armazenamento do host

Um produto de armazenamento é suportado se for gerenciável por meio de um hipervisor suportado. O Suporte Citrix auxilia apenas esses fornecedores de produtos de armazenamento na solução de problemas e na resolução de problemas, e na documentação desses problemas e soluções no Centro de Conhecimento, conforme necessário.

Ao provisionar máquinas, os dados são classificados por tipo:

- Sistema operacional (SO): inclui imagens
- Dados temporários: incluem todos os dados não persistentes gravados em máquinas provisionadas por MCS, arquivos de paginação do Windows e quaisquer dados sincronizados com o ShareFile. Esses dados são descartados cada vez que uma máquina é reiniciada. Se a imagem base incluir dados de perfil de usuário, esses dados permanecerão persistentes. Se uma solução centralizada de perfil de usuário estiver em uso, os dados de perfil de usuário

serão sincronizados com o armazenamento de perfil externo. Os dados de perfil de usuário armazenados em cache localmente são descartados a cada reinício da máquina.

A alocação de recursos de armazenamento distintos para diferentes tipos de dados pode minimizar a carga do sistema e aprimorar o desempenho de IOPS (Operações de Entrada/Saída por Segundo) em cada dispositivo de armazenamento. Essa alocação estratégica faz uso ideal dos recursos disponíveis do host. Além disso, permite a seleção do meio de armazenamento mais adequado com base nas necessidades específicas de cada tipo de dado, como maior persistência ou resiliência para certos tipos de dados.

- Opções de armazenamento compartilhado e local: Os recursos de armazenamento podem ser centralizados, ou seja, separados de qualquer host e usados por todos os hosts, ou localizados em um hipervisor específico. As opções centralizadas incluem volumes compartilhados de cluster do Windows, que podem ou não ter armazenamento adicional anexado, ou appliances de fornecedores de armazenamento. As soluções de armazenamento centralizado podem oferecer recursos avançados para otimizações, por exemplo, caminhos de controle de armazenamento específicos do hipervisor e acesso direto a plug-ins.
- Benefícios e desvantagens do armazenamento local: Armazenar dados temporários localmente evita o acesso à rede para acessar o armazenamento compartilhado, reduzindo assim a carga de IOPS nos recursos compartilhados. Embora o armazenamento centralizado possa ser mais caro, usar o armazenamento local pode ser uma alternativa econômica. No entanto, esses benefícios podem ser ponderados em relação à disponibilidade de armazenamento suficiente nos servidores do hipervisor.

Armazenamento compartilhado por hipervisores

O método de armazenamento compartilhado por hipervisores armazena dados que precisam de persistência de longo prazo de forma centralizada, fornecendo backup e gerenciamento centralizados. Esse armazenamento contém os discos do sistema operacional.

Ao selecionar este método, você pode escolher se deseja usar armazenamento local (em servidores no mesmo pool de hipervisores) para dados temporários da máquina. Esses dados não exigem persistência ou tanta resiliência quanto os dados no armazenamento compartilhado. Isso é chamado de *cache de dados temporários*. O disco local ajuda a reduzir o tráfego para o armazenamento principal do sistema operacional. Este disco é limpo após cada reinicialização da máquina. O disco é acessado por meio de um cache de memória write-through. Lembre-se de que, se você usar armazenamento local para dados temporários, o VDA provisionado estará vinculado a um host de hipervisor específico. Se esse host falhar, a VM não poderá iniciar.

Exceção: Se você usar Volumes de Armazenamento Clusterizados (CSV), o Microsoft System Center Virtual Machine Manager não permitirá que discos de cache de dados temporários sejam criados no armazenamento local.

Se você armazenar dados temporários localmente, poderá habilitar e configurar valores não padrão para o disco de cache e o tamanho da memória de cada VM ao criar um catálogo de máquinas que usa essa conexão. No entanto, os valores padrão são conforme o tipo de conexão e são suficientes para a maioria dos casos.

O hipervisor também pode fornecer tecnologias de otimização por meio de cache de leitura em memória das imagens de disco localmente. Por exemplo, o XenServer oferece o IntelliCache. Isso também pode reduzir o tráfego de rede para o armazenamento central.

Armazenamento local ao hipervisor

O método de armazenamento local ao hipervisor armazena dados localmente no hipervisor. Com este método, imagens e outros dados do sistema operacional são transferidos para todos os hipervisores usados no site, tanto para a criação inicial da máquina quanto para futuras atualizações de imagem. Isso resulta em tráfego significativo na rede de gerenciamento. As transferências de imagem também consomem muito tempo, e as imagens ficam disponíveis para cada host em um momento diferente.

Criar uma conexão e recursos

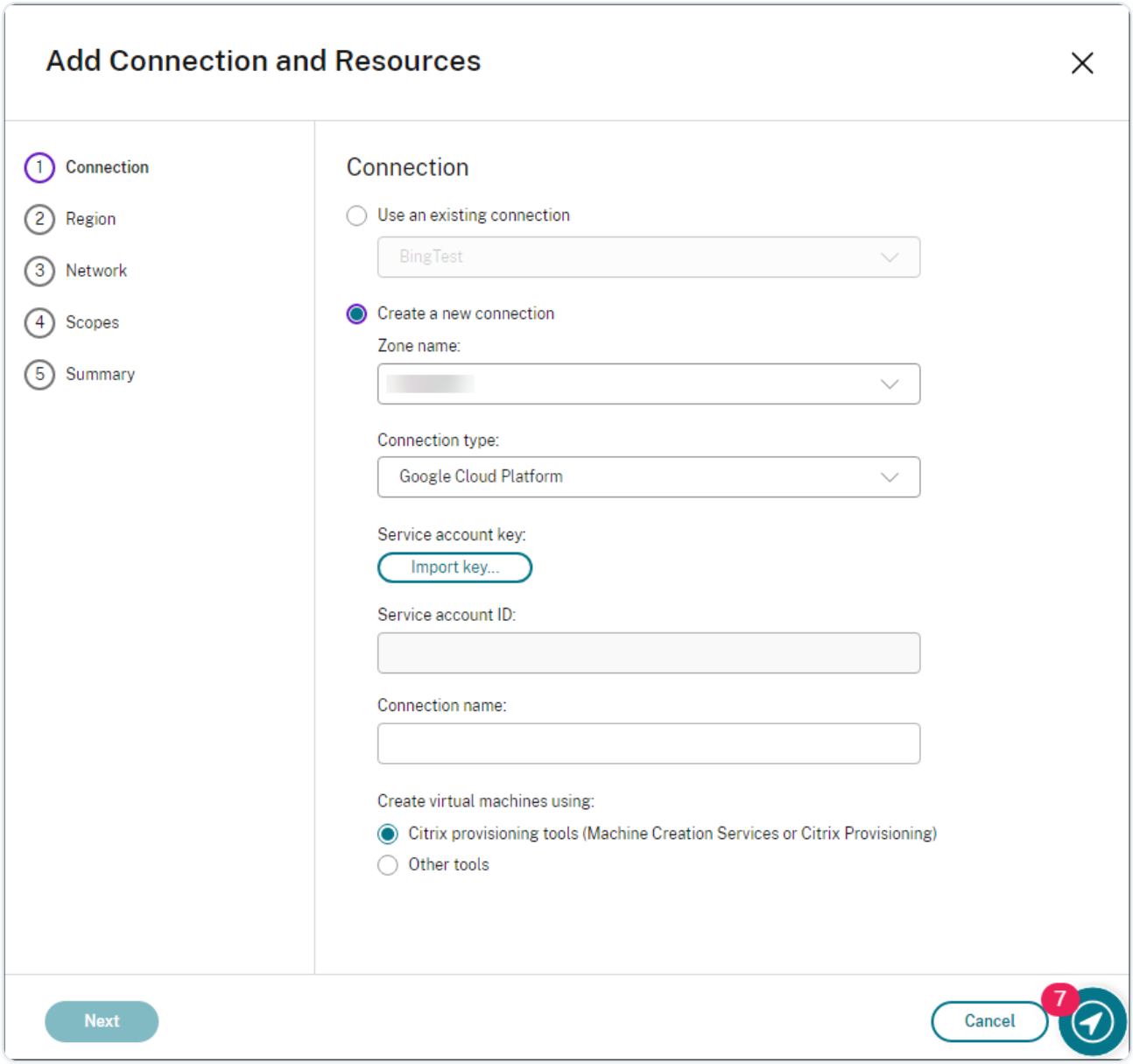
> **Importante:**
>
> Os recursos do host (armazenamento e rede) em seu local de recurso devem estar disponíveis antes de você criar uma conexão.

1. Faça login no Citrix Cloud.
2. No bloco **DaaS**, clique em **Gerenciar** para abrir o Studio.
3. Selecione **Hospedagem** no painel esquerdo.
4. Clique em **Adicionar Conexões e Recursos** na barra de ações.
5. O assistente o guia pelo processo de configuração descrito nas etapas a seguir. O conteúdo específico da página depende do tipo de conexão selecionado. Após concluir as etapas em cada página, selecione **Avançar** até chegar à página **Resumo**.

Nota:

O conteúdo de cada página no assistente varia de acordo com o tipo de conexão que você selecionou.

Etapa 1. Conexão



Na página **Conexão**:

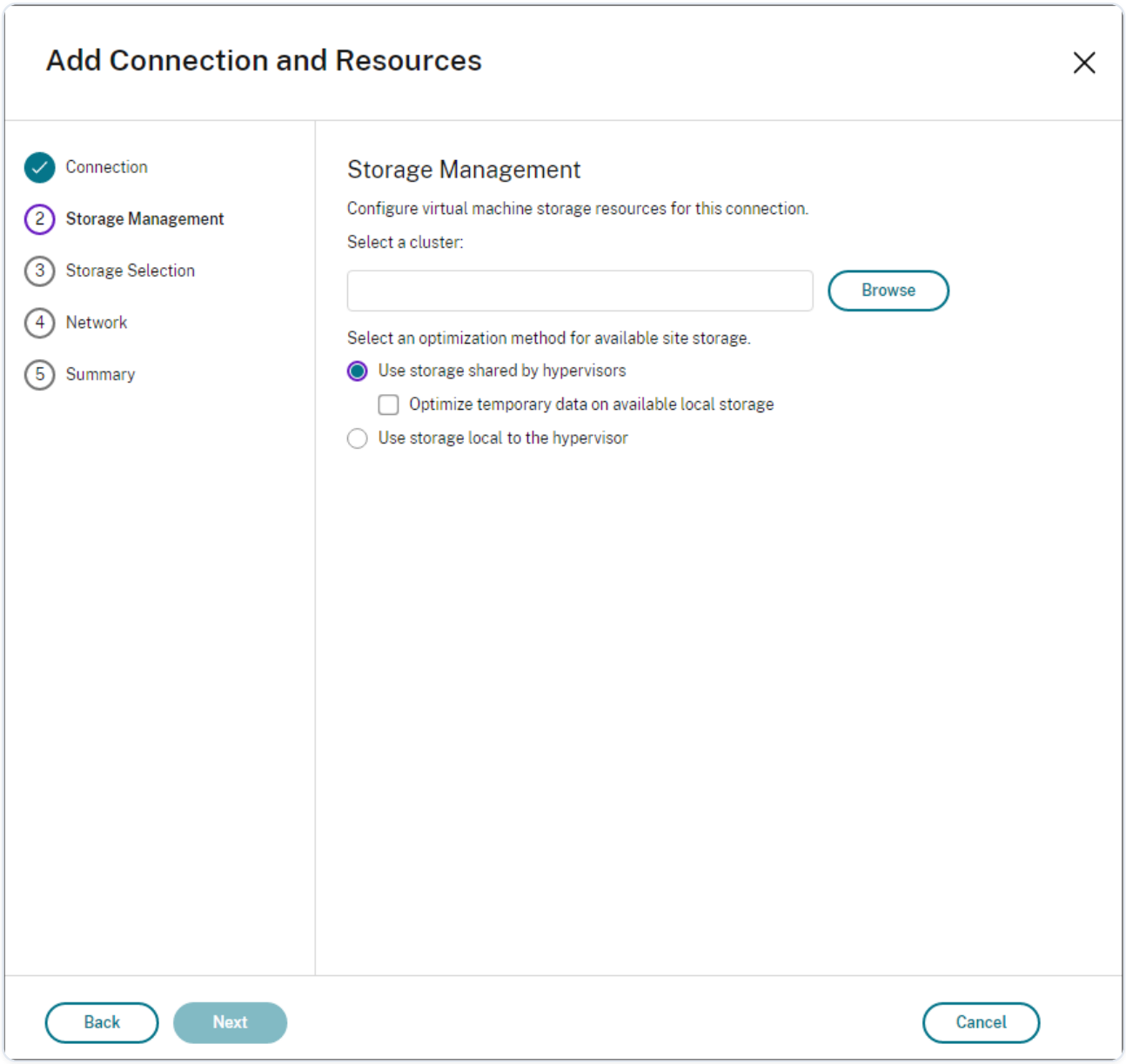
- Para criar uma nova conexão, selecione **Criar uma nova Conexão**. Para criar um recurso para uma conexão existente, selecione **Usar uma Conexão existente** e, em seguida, escolha a conexão relevante.
- Selecione uma zona no campo **Nome da zona**. As opções são todos os locais de recursos que você configurou.

- Selecione um hipervisor ou serviço de nuvem no campo **Tipo de conexão**. As opções incluem todos os hipervisores e serviços de nuvem compatíveis com a Citrix:
  - Para um local de recurso sem Cloud Connectors acessíveis, apenas hipervisores e serviços de nuvem que suportam implantações sem conector estão disponíveis.
  - Para um local de recurso com Cloud Connectors acessíveis, apenas hipervisores e serviços de nuvem que têm seus plug-ins instalados corretamente nesses conectores estão disponíveis.

  Alternativamente, você pode usar o comando PowerShell `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false ou true para obter a lista de hipervisores e serviços de nuvem disponíveis.
- Insira um nome de conexão. Este nome aparece na exibição **Hospedagem**.
- Escolha uma ferramenta para criar máquinas virtuais.

> **Nota:**
>
> As informações na página **Conexão** diferem dependendo do tipo de host ou conexão que você está usando. Por exemplo, ao usar o Azure Resource Manager, você pode escolher entre uma entidade de serviço ou uma identidade gerenciada. Para obter detalhes, consulte Conexão com o Microsoft Azure.

Etapa 2. Gerenciamento de armazenamento



Para obter informações sobre tipos e métodos de gerenciamento de armazenamento, consulte Armazenamento do host.

Se você estiver configurando uma conexão com um host Hyper-V ou VMware, navegue até e selecione um nome de cluster. Outros tipos de conexão não solicitam um nome de cluster.

Selecione um método de gerenciamento de armazenamento: armazenamento compartilhado por hipervisores ou armazenamento local ao hipervisor.

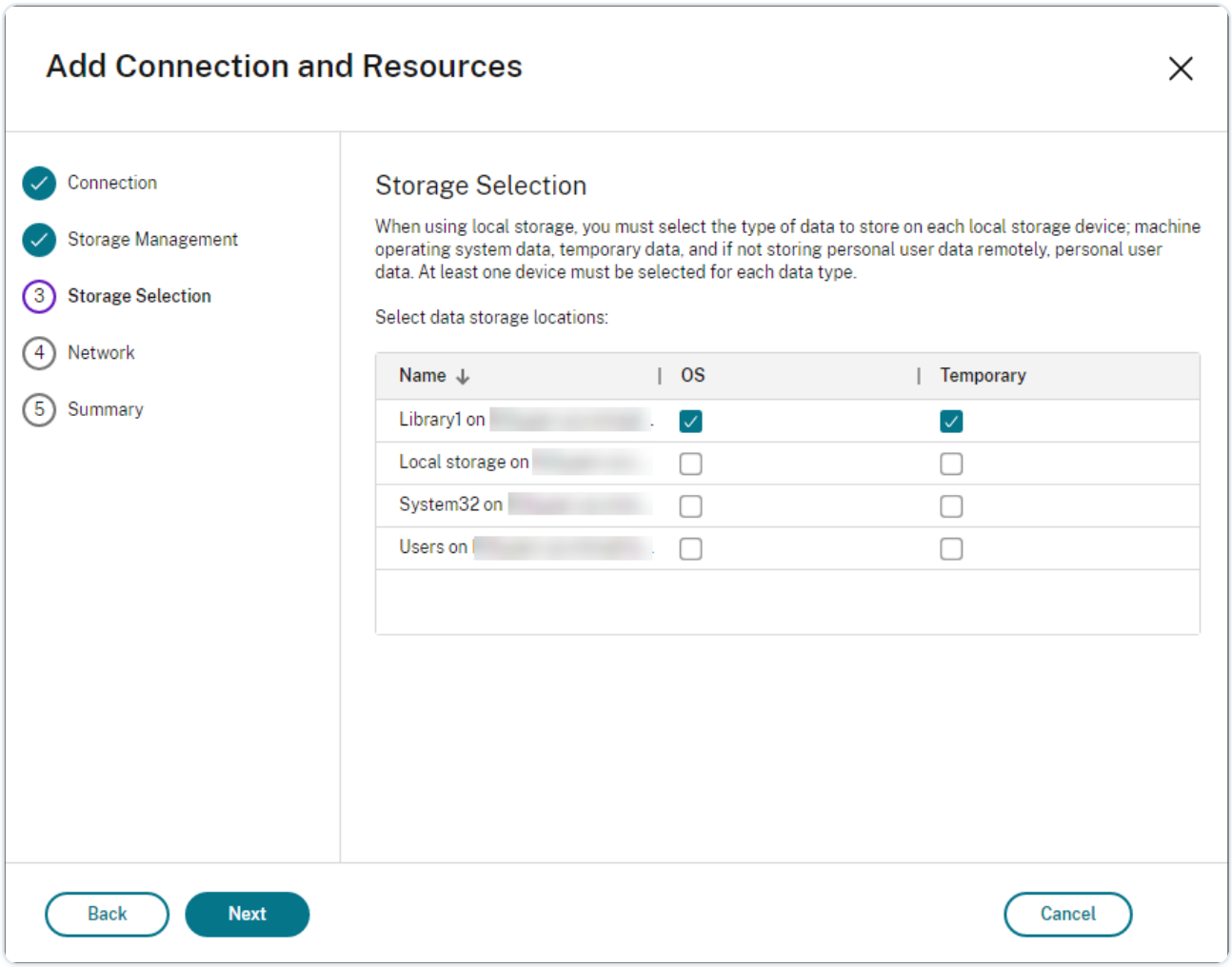
Para obter mais informações, consulte Armazenamento compartilhado por hipervisores e Armazenamento local ao hipervisor.

Se você usar armazenamento compartilhado em um pool XenServer, indique se deseja usar o IntelliCache para reduzir a carga no dispositivo de armazenamento compartilhado. Consulte Usar IntelliCache para conexões XenServer.

Nota:

Em ambientes de virtualização XenServer®, VMware e SCVMM, você pode ter o disco de cache de write-back (WBC) no mesmo local de armazenamento do disco do SO. Para isso, não selecione **Otimizar dados temporários no armazenamento local disponível**.

Etapa 3. Seleção de armazenamento



Para obter mais informações sobre a seleção de armazenamento, consulte Armazenamento do host.

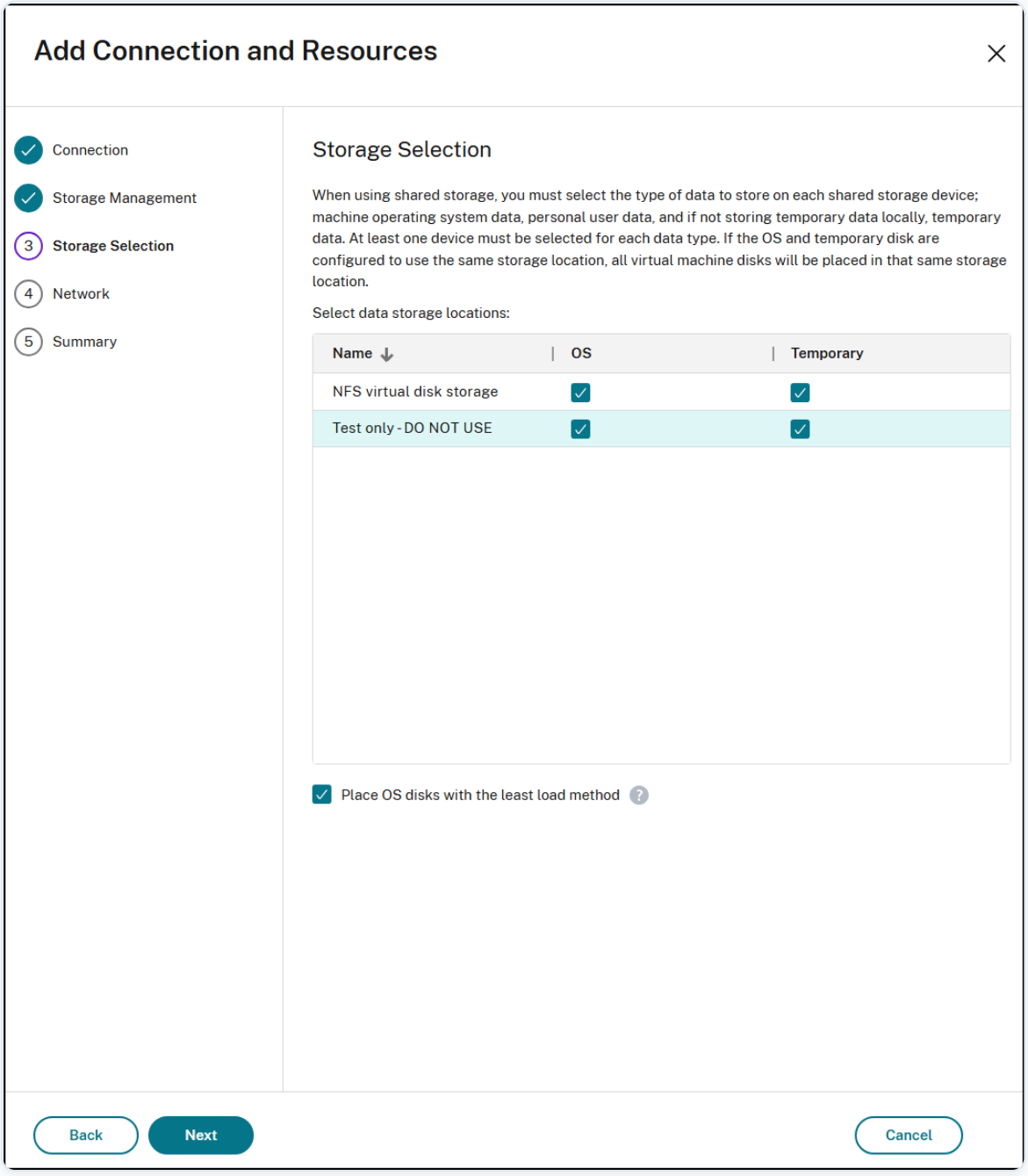
Selecione pelo menos um dispositivo de armazenamento do host para cada tipo de dados disponível. O método de gerenciamento de armazenamento que você selecionou na página anterior afeta quais tipos de dados estão disponíveis para seleção nesta página. Você deve

selecionar pelo menos um dispositivo de armazenamento para cada tipo de dados suportado antes de prosseguir para a próxima página do assistente.

Nota:

- Em ambientes de virtualização XenServer, VMware e SCVMM, o MCS coloca o disco de cache de write-back (WBC) no mesmo local de armazenamento que o disco do SO se você configurar a lista de armazenamento de SO disponível da mesma forma que a lista de armazenamento temporário disponível.
- Se você selecionar pelo menos dois ou mais locais de armazenamento de dados do SO, a opção **Otimizar balanceamento de carga de armazenamento com método de menor carga** aparecerá. Esta opção permite que você escolha o repositório de

armazenamento menos carregado para alocação de disco.



- A página **Resumo** indica se a opção está **Ativada** ou **Desativada**, dependendo da sua seleção. O painel **Detalhes** exibe as alterações no método de alocação de armazenamento. Você pode ajustá-lo usando a opção **Editar armazenamento** na página **Armazenamento do SO**.

Você pode obter mais opções de configuração na página **Seleção de Armazenamento** se escolher **Usar armazenamento compartilhado por hipervisores** e selecionar **Otimizar dados temporários no armazenamento local disponível** na página **Gerenciamento de**

> **Armazenamento**. Por exemplo, você pode selecionar quais dispositivos de armazenamento local (no mesmo pool de hipervisores) usar para dados temporários.

O número de dispositivos de armazenamento atualmente selecionados é mostrado (no gráfico, "1 dispositivo de armazenamento selecionado"). Ao passar o mouse sobre essa entrada, os nomes dos dispositivos selecionados aparecem (a menos que nenhum dispositivo esteja configurado).

1. Selecione **Selecionar** para alterar os dispositivos de armazenamento a serem usados.
2. Na caixa de diálogo **Selecionar Armazenamento**, selecione ou desmarque as caixas de seleção do dispositivo de armazenamento e, em seguida, selecione **OK**.

Etapa 4. Região

> **Nota:**

> A página **Região** aparece apenas para alguns tipos de host.

> A seleção da região indica onde as VMs serão implantadas. Idealmente, escolha uma região próxima de onde os usuários acessarão seus aplicativos.

Etapa 5. Rede

Insira um nome para os recursos. Este nome identifica a combinação de armazenamento e rede associada à conexão.

Selecione uma ou mais redes que as VMs usarão.

Alguns tipos de conexão (como Azure Resource Manager) também listam sub-redes que as VMs usarão. Selecione uma ou mais sub-redes.

Etapa 6. Resumo

Revise suas seleções. Se quiser fazer alterações, retorne às páginas anteriores do assistente. Ao concluir sua revisão, selecione **Concluir**.

> **Nota:**

- Se você armazenar dados temporários localmente, poderá configurar valores não padrão para o armazenamento de dados temporários ao criar o catálogo que contém as máquinas que usam essa conexão.
- Um escopo não é exibido para administradores de acesso total. Para obter mais informações, consulte Administradores, funções e escopos.

Editar configurações de conexão

Você não pode usar este procedimento para:

- Renomear uma conexão ou criar uma nova conexão.
- Alterar as configurações de GPU para uma conexão. Os catálogos que acessam esse recurso devem usar uma imagem apropriada específica para GPU. Portanto, se você quiser alterar as configurações de GCP, crie uma nova conexão em vez de editar uma conexão existente.

Editar uma conexão

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e, em seguida, selecione **Editar Conexão** na barra de ações.
3. Use a página **Propriedades da Conexão** para alterar o endereço e as credenciais da conexão. Altere o endereço somente se a máquina host atual tiver um novo endereço. Inserir um endereço para uma máquina diferente interrompe os catálogos de máquinas da conexão.
   - Selecione **Editar configurações…** e, em seguida, insira as novas informações.
   - Para especificar os servidores de alta disponibilidade para uma conexão XenServer, selecione **Editar servidores...** e selecione os servidores. A Citrix recomenda que você selecione todos os servidores no pool para permitir a comunicação com o XenServer caso o mestre do pool falhe.

     Nota:

     Se você estiver usando HTTPS e quiser configurar servidores de alta disponibilidade, não instale um certificado curinga para todos os servidores em um pool. É necessário um certificado individual para cada servidor. Para obter mais informações, consulte Criar uma conexão com o XenServer.

4. Use a página **Avançado** para editar as configurações para especificar um número máximo de ações simultâneas (ou máquinas concorrentes) por conexão de hospedagem. Essas configurações podem ajudar quando as configurações de gerenciamento de energia permitem que muitas ou poucas máquinas iniciem ao mesmo tempo. Cada tipo de conexão tem valores padrão específicos que são apropriados para a maioria dos casos. Geralmente, eles não precisam ser alterados.

    - As configurações **Ações simultâneas (todos os tipos)** e **Atualizações de inventário de vDisk pessoal simultâneas** especificam dois valores: um número absoluto máximo que pode ocorrer simultaneamente nesta conexão e uma porcentagem máxima de todas as máquinas que usam esta conexão. Você deve especificar valores absolutos e percentuais. O limite real aplicado é o menor dos valores.

      Por exemplo, em uma implantação com 34 máquinas, se **Ações simultâneas (todos os tipos)** for definido como um valor absoluto de 10 e um valor percentual de 10, o limite real aplicado é 3 (ou seja, 10% de 34 arredondado para o número inteiro mais próximo, que é menor que o valor absoluto de 10 máquinas).
    - O **Número máximo de novas ações por minuto** é um número absoluto. Não há valor percentual.
    - Insira informações em **Opções de conexão** somente sob a orientação de um representante do Suporte Citrix.

5. Use a página **Escopos** para selecionar um ou mais escopos para este host.

    > **Nota:**
    >
    > Um escopo não é exibido para administradores de acesso total. Por definição, esses administradores podem acessar todos os objetos de serviços inscritos e do Citrix Cloud gerenciados pelo cliente.
    >
    > Para obter mais informações, consulte Administradores, funções e escopos.

6. Use a página **Locatários Compartilhados** para adicionar locatários e assinaturas que compartilham a Galeria de Computação do Azure com a assinatura desta conexão.

    a. Insira o **Segredo do aplicativo** para o aplicativo associado a esta conexão. Com essas informações, você pode autenticar no Azure. Recomendamos que você altere as chaves regularmente para garantir a segurança.

b. Adicione locatários e assinaturas compartilhados. Você pode adicionar até oito locatários compartilhados. Para cada locatário, você pode adicionar até oito assinaturas.

7. Clique em **Salvar** e **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Ativar ou desativar o modo de manutenção para uma conexão

Ativar o modo de manutenção para uma conexão impede que qualquer nova ação de energia afete qualquer máquina armazenada na conexão. Os usuários não podem se conectar a uma máquina quando ela está no modo de manutenção. Se os usuários já estiverem conectados, o modo de manutenção entrará em vigor quando eles fizerem logoff.

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão. Para ativar o modo de manutenção, selecione **Ativar Modo de Manutenção** na barra de ações. Para desativar o modo de manutenção, selecione **Desativar Modo de Manutenção**.

Você também pode ativar ou desativar o modo de manutenção para máquinas individuais. Você pode ativar ou desativar o modo de manutenção para máquinas em catálogos de máquinas ou grupos de entrega.

Excluir uma conexão

> **Cuidado:**

> A exclusão de uma conexão pode resultar na exclusão de um grande número de máquinas e na perda de dados. Certifique-se de que os dados do usuário nas máquinas afetadas estejam com backup ou não sejam mais necessários.

> Antes de excluir uma conexão, certifique-se de que:

- Todos os usuários fizeram logoff das máquinas armazenadas na conexão.
- Nenhuma sessão de usuário desconectada está em execução.
- O modo de manutenção está ativado para máquinas agrupadas e dedicadas.
- Todas as máquinas em catálogos de máquinas usadas pela conexão estão desligadas.

Um catálogo de máquinas torna-se inutilizável quando você exclui uma conexão que o catálogo referencia. Se esta conexão for referenciada por um catálogo, você poderá excluir o catálogo. Antes de excluir um catálogo, certifique-se de que ele não seja usado por outras conexões.

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e então selecione **Excluir Conexão** na barra de ações.
3. Se esta conexão tiver máquinas armazenadas nela, será perguntado se deseja excluir as máquinas. Se elas forem excluídas, especifique o que fazer com as contas de computador do Active Directory associadas.

Renomear uma conexão

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e então selecione **Renomear Conexão**.

Testar uma conexão

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e então selecione **Testar Conexão**.

Testar Certificado TLS

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Clique com o botão direito na conexão para a qual você deseja confiar novamente no certificado com um símbolo de aviso e selecione **Testar Confiança do Certificado TLS**.
3. Insira a senha na janela subsequente e clique em **Salvar**.
    a. Se o certificado precisar ser novamente confiável, uma caixa de diálogo de aviso é exibida com uma opção para confiar no certificado.
    b. Se o certificado já for confiável, uma caixa de diálogo de sucesso é exibida informando que o certificado é confiável.

Exibir detalhes da máquina em uma conexão

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e, em seguida, selecione **Exibir Máquinas** na barra de ações.

O painel superior lista as máquinas acessadas pela conexão. Selecione uma máquina para ver seus detalhes no painel inferior. Os detalhes da sessão também são fornecidos para sessões abertas.

Use o recurso de pesquisa para encontrar máquinas rapidamente. Selecione uma pesquisa salva na lista na parte superior da janela ou crie uma nova pesquisa. Você pode pesquisar digitando todo ou parte do nome da máquina, ou pode criar uma expressão para usar em uma pesquisa avançada. Para criar uma expressão, selecione **Desdobrar** e, em seguida, selecione nas listas de propriedades e operadores.

Gerenciar máquinas em uma conexão

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione uma conexão e, em seguida, selecione **Exibir Máquinas** na barra de ações.
3. Selecione uma das seguintes opções na barra de ações. Algumas ações podem não estar disponíveis, dependendo do estado da máquina e do tipo de conexão do host.

    - **Iniciar:** Inicia a máquina se ela estiver desligada ou suspensa.
    - **Suspender:** Pausa a máquina sem desligá-la e atualiza a lista de máquinas.
    - **Desligar:** Solicita ao sistema operacional que desligue.
    - **Forçar desligamento:** Desliga a máquina à força e atualiza a lista de máquinas.
    - **Reiniciar:** Solicita ao sistema operacional que desligue e, em seguida, inicie a máquina novamente. Se o sistema operacional não puder cumprir, a área de trabalho permanecerá em seu estado atual.
    - **Habilitar modo de manutenção:** Interrompe temporariamente as conexões com uma máquina. Os usuários não podem se conectar a uma máquina neste estado. Se os usuários estiverem conectados, o modo de manutenção entrará em vigor quando eles fizerem logoff. (Você também pode ativar ou desativar o modo de manutenção para todas as máquinas acessadas por meio de uma conexão, conforme descrito anteriormente.)
    - **Remover do Grupo de Entrega:** Remover uma máquina de um Grupo de Entrega não a exclui do catálogo de máquinas que o Grupo de Entrega usa. Você só pode remover uma máquina quando nenhum usuário estiver conectado a ela. Ative o modo de manutenção para impedir temporariamente que os usuários se conectem enquanto você remove a máquina.
    - **Excluir:** Ao excluir uma máquina, os usuários não terão mais acesso a ela, e a máquina será excluída do catálogo de máquinas. Antes de excluir uma máquina, certifique-se de que todos os dados do usuário estejam salvos ou não sejam mais necessários. Você só pode excluir uma máquina quando nenhum usuário estiver conectado a ela. Ative o modo de manutenção para impedir temporariamente que os usuários se conectem enquanto você estiver excluindo a máquina.

Para ações que envolvem o desligamento da máquina, se a máquina não desligar em 10 minutos, ela será desligada. Se o Windows tentar instalar atualizações durante o desligamento, há o risco de a máquina ser desligada antes que as atualizações sejam concluídas.

Editar armazenamento

Você pode exibir o status dos servidores que são usados para armazenar o sistema operacional, dados temporários e pessoais (PvD) para VMs que usam uma conexão. Você também pode especificar quais servidores usar para o armazenamento de cada tipo de dado.

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e, em seguida, selecione **Editar Armazenamento** na barra de ações.
3. No painel esquerdo, selecione o tipo de dados: sistema operacional ou temporário.
4. Marque ou desmarque as caixas de seleção para um ou mais dispositivos de armazenamento para o tipo de dados selecionado.
5. Selecione **OK**.

Cada dispositivo de armazenamento na lista inclui seu nome e status de armazenamento. Os valores de status de armazenamento válidos são:

- **Em uso**: O armazenamento está sendo usado para criar máquinas.
- **Substituído**: O armazenamento está sendo usado apenas para máquinas existentes. Nenhuma máquina nova é adicionada a este armazenamento.
- **Não em uso**: O armazenamento não está sendo usado para criar máquinas.

Se você desmarcar a caixa de seleção de um dispositivo que está atualmente **Em uso**, seu status muda para **Substituído**. As máquinas existentes continuarão a usar esse dispositivo de armazenamento (e podem gravar dados nele). Assim, esse local pode ficar cheio mesmo depois de parar de ser usado para criar máquinas.

Detectar recursos órfãos do Azure

Recursos órfãos são recursos não utilizados presentes no sistema e podem levar a despesas desnecessárias.

Além dos administradores de nuvem, quaisquer funções recém-criadas com a permissão **Usar Conexão de Host para Detectar Recursos Órfãos no Hypervisor** em **Hosts** poderão detectar recursos órfãos.

Este recurso permite detectar os recursos órfãos do Azure nos hosts do seu site de nuvem.

Siga as etapas no Citrix DaaS™:

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione uma conexão e, em seguida, selecione **Detectar Recursos Órfãos** na barra de ações. A caixa de diálogo **Detectar Recursos Órfãos** exibe o relatório de recursos órfãos.
3. Para visualizar o relatório de recursos órfãos, selecione **Visualizar Relatório**.

Alternativamente, você pode detectar recursos órfãos do Azure usando o PowerShell. Para obter mais informações, consulte Recuperar uma lista de recursos órfãos.

Para entender as razões por trás dos recursos órfãos e aprender como prosseguir, consulte Gerenciar recursos órfãos do Azure de forma eficiente com o Citrix.

Temporizadores de conexão

Você pode usar as configurações de política do Citrix para configurar três temporizadores de conexão:

- **Temporizador máximo de conexão:** Determina a duração máxima de uma conexão ininterrupta entre um dispositivo de usuário e um desktop virtual. Use as configurações de política **Temporizador de conexão de sessão** e **Intervalo do temporizador de conexão de sessão**.
- **Temporizador de inatividade da conexão:** Determina por quanto tempo uma conexão ininterrupta de dispositivo de usuário com um desktop virtual é mantida se não houver entrada do usuário. Use as configurações de política **Temporizador de inatividade da sessão** e **Intervalo do temporizador de inatividade da sessão**.
- **Temporizador de desconexão**: Determina por quanto tempo um desktop virtual desconectado e bloqueado pode permanecer bloqueado antes que a sessão seja encerrada. Use as configurações de política **Temporizador de sessão desconectada** e **Intervalo do temporizador de sessão desconectada**.

Ao atualizar qualquer uma dessas configurações, certifique-se de que elas sejam consistentes em toda a sua implantação.

Consulte a documentação de configurações de política para obter mais informações.

Editar redes de recursos

Você pode alterar as redes de uma conexão. Faça o seguinte:

1. Vá para **Hospedagem**.

2. Selecione os recursos de destino na conexão e, em seguida, selecione **Editar Rede** na barra de ações.
3. Selecione uma ou mais redes para as máquinas virtuais usarem.
4. Clique em **Salvar** para salvar suas alterações e sair.

Excluir, renomear ou testar recursos

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione os recursos de destino na conexão e, em seguida, selecione a entrada apropriada na barra de ações:
    - **Excluir Recursos**
    - **Renomear Recursos**
    - **Testar Recursos**

Opção de local de armazenamento flexível para VMs

As VMs em um catálogo de máquinas recebem vários serviços de armazenamento (SR). Para equilibrar a alocação de VM em diferentes armazenamentos, você tem duas opções:

- **Método de alocação round robin aprimorado**: Em vez de sempre começar do mesmo SR fixo, o MCS inicia a alocação do SR logo após o último SR usado.
- **Método de alocação baseado na menor carga**: Coloca as VMs na menor carga atual, determinada comparando o número total de VMs em cada SR dentro do mesmo catálogo de máquinas. Por exemplo, se um catálogo de máquinas contém 100 VMs distribuídas da seguinte forma: 20 VMs no SR1, 30 VMs no SR2 e 50 VMs no SR3, as novas VMs são alocadas primeiro no SR1. Este método garante que a carga entre SR1, SR2 e SR3 seja balanceada.

Este recurso é:

- Aplicável a todos os hipervisores locais (VMware, XenServer e Hyper-V)
- Aplicável apenas ao armazenamento de disco do SO.
- Não aplicável às VMs existentes

Para implementar a opção de alocação baseada em carga, adicione a propriedade personalizada `Name="StorageBalanceType"` `Value="VMCountBasedLeastLoad` ao criar ou atualizar uma

conexão de host. Se você não usar esta propriedade e valor personalizados, por padrão, o método round robin aprimorado será aplicado.

Por exemplo:

- Ao criar uma conexão de host:

```
New-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>"
-HypervisorConnectionName "Xen-Connection" -NetworkPath @("XDHyp:
\Connections\Xen-Connection\Network 0.network") -Path @("XDHyp:
\HostingUnits\XS-Network") -PersonalvDiskStoragePath @() -RootPath
"XDHyp:\Connections\Xen-Connection\" -StoragePath @("XDHyp:
\Connections\Xen-Connection\NFS virtual disk storage.storage")
```

- Ao atualizar uma conexão de host:

```
Set-Item  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>" -Path @("XDHyp:
\HostingUnits\XS-Network")
```

Recuperar uma lista de recursos órfãos

Você pode obter uma lista de recursos órfãos que são criados pelo MCS, mas não são mais rastreados pelo MCS. Isso é atualmente aplicável a ambientes Azure. Para obter a lista, você pode usar comandos PowerShell. Você pode filtrar usando conexões.

Por padrão, as funções de **Administrador Completo** e **Administrador de Nuvem** têm esta permissão atribuída. Para permitir que outras funções executem esta ação, atribua a elas a permissão **Usar Conexão de Host para Detectar Recursos Órfãos no Hipervisor** em **Hosts**. Para obter mais informações, consulte Criar e gerenciar funções.

> **Nota:**

> O comando PowerShell é rejeitado se qualquer provisionamento ou atualização de imagem estiver em andamento.

Limitações

- Para evitar o reconhecimento incorreto de recursos órfãos, não ligue as VMs enquanto estiver filtrando recursos órfãos.
- Cerca de 2.000 registros são exibidos como órfãos se houver uma possível carga de trabalho pesada.

Exibir a lista de recursos órfãos

Para exibir a lista de recursos órfãos

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Execute os seguintes comandos:
   a. Obtenha o uid da conexão. O uid da conexão é o valor do atributo HypervisorConnectionUid.

   ```
   Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
   'Azure*' }"
   ```

   b. Obtenha a lista de recursos órfãos.

   ```
   get-provorphanedresource

   -HypervisorConnectionUid <connection uid>
   ```

Exibir a lista de recursos órfãos de um ID de assinatura

Para exibir a lista de recursos órfãos de um ID de assinatura:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Execute os seguintes comandos:
   a. Encontre o uid da conexão usando o ID da assinatura. O uid da conexão é o valor do atributo HypervisorConnectionUid.

```
Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
-match '<subscriptionId>' }
```

b. Obtenha a lista de recursos órfãos.

```
get-provorphanedresource -HypervisorConnectionUid <connection uid>
```

Nota:

Verifique os recursos cuidadosamente antes de excluí-los.

Usar as configurações do servidor proxy WinHttp (netsh) para conexão de hospedagem

Este aprimoramento de recurso permite que as conexões de hospedagem usem as configurações do servidor proxy WinHttp (netsh) com a conexão de hospedagem. Isso permite uma configuração de proxy mais simples e também garante o uso consistente do proxy entre o Cloud Connector e as conexões de host.

Este recurso é aplicável aos seguintes ambientes de virtualização:

- Nutanix
- HPE Moonshot
- Red Hat OpenShift

Casos de uso

- Exemplo 1: Nenhuma propriedade personalizada é definida na conexão de hospedagem

  A conexão de hospedagem não lerá nenhuma configuração de proxy na máquina e tentará se conectar ao hipervisor sem um proxy.

- Exemplo 2: A propriedade personalizada é definida na conexão de hospedagem com valor = True

  A conexão de hospedagem lerá apenas as configurações de proxy WinHttp e usará as configurações de proxy, se presentes. Se não estiverem presentes, nenhuma configuração de proxy será usada para a conexão de hospedagem.

- Exemplo 3: A propriedade personalizada é definida na conexão de hospedagem com valor = False

  A conexão de hospedagem não lerá nenhuma configuração de proxy na máquina e tentará se conectar ao hipervisor sem um proxy.

Alterações no fluxo de trabalho ou processo existente

- Para usar o servidor proxy WinHttp (netsh) configurado nos Cloud Connectors para a conexão de hospedagem, agora você pode incluir esta propriedade personalizada com a conexão de hospedagem.

```
<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />
```

- Quando esta propriedade personalizada é definida como `True`, as chamadas de API para o hipervisor são roteadas através do servidor proxy WinHttp configurado na máquina por meio do comando netsh winhttp set proxy.
- Quando esta propriedade personalizada é definida como `False`, ou esta propriedade personalizada não é definida, as chamadas de API ignorarão todos os servidores proxy (incluindo o proxy WinINet e o proxy .net) configurados nos Cloud Connectors.

Pré-requisito

Antes de definir a propriedade personalizada ao criar a conexão de host usando o PowerShell, certifique-se de configurar o proxy WinHTTP em todos os Citrix Cloud Connectors no Local do Recurso.

Etapas de configuração

Para criar uma nova conexão de hospedagem para usar as configurações de proxy WinHttp via CLI:

```
$CustomProperties = "<CustomProperties  xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<!-- Include any other hypervisor specific custom properties here -->

<Property xsi:type=`"StringProperty`"
Name=`"UseSystemProxyForHypervisorTrafficOnConnectors`" Value=`"True`" />
```

```
</CustomProperties>"



New-Item -ConnectionType $ConnectionType -HypervisorAddress @('https://
hypervisorhost1.example.com') -Path @('XDHyp:\Connections\
$ConnectionName') -Password $Password -UserName $User -CustomProperties
$CustomProperties
```

Para definir a propriedade personalizada em uma conexão de hospedagem existente:

1. Copie as propriedades personalizadas existentes da conexão de host, se houver.

   ```
   dir XDHyp:\Connections
   ```

2. Copie as propriedades personalizadas para sua conexão de host e adicione o seguinte, e salve-o em uma variável.

   ```
   $CustomProperties

   <Property xsi:type=`"StringProperty`"
   Name=`"UseWinHttpProxyForHypervisorTraffic`" Value=`"True`" />
   ```

   Exemplo:

   ```
   $CustomProperties = "<CustomProperties xmlns=`"http://
   schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
   www.w3.org/2001/XMLSchema-instance`">

   <Property xsi:type=`"IntProperty`"
   Name=`"MaximumConcurrentProvisioningOperations`" Value=`"100`"/
   ><Property xsi:type=`"StringProperty`"
   Name=`"UseSystemProxyForHypervisorTrafficOnConnectors`"
   Value=`"True`" />

   </CustomProperties>"
   ```

   Se a propriedade personalizada existente estava vazia, defina a propriedade personalizada:

```
$CustomProperties = "<CustomProperties  xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`"
Name=`"UseSystemProxyForHypervisorTrafficOnConnectors`"
Value=`"True`" />

</CustomProperties>"
```

3. Execute o comando `Set-Item` para atualizar a conexão de hospedagem existente.

```
Set-Item -CustomProperties $CustomProperties -LiteralPath @("XDHyp:
\Connections\$ConnectionName") -PassThru -UserName $User
-SecurePassword $Password
```

Onde ir em seguida

- Para obter informações sobre a conexão com tipos de host específicos, consulte:
  - Conexão com AWS
  - Conexão com ambientes de nuvem do Google
  - Conexão com Microsoft Azure
  - Conexão com Microsoft System Center Virtual Machine Manager
  - Conexão com Nutanix
  - Conexão com soluções de nuvem e parceiros Nutanix
  - Conexão com VMware
  - Conexão com soluções de nuvem e parceiros VMware
  - Conexão com XenServer

Se você estiver no processo de implantação inicial, crie um catálogo de máquinas.

Conexão com Amulet Hotkey CoreStation

Criar e gerenciar conexões e recursos descreve os assistentes gerais para criar uma conexão. As informações a seguir cobrem detalhes específicos do Amulet Hotkey CoreStation. Atualmente, você pode criar uma conexão com o Amulet Hotkey CoreStation usando comandos PowerShell.

> **Nota:**
>
> Antes de criar uma conexão com o Amulet Hotkey CoreStation, você precisa primeiro concluir a configuração da sua conta Amulet Hotkey CoreStation. Consulte Ambientes de virtualização do Amulet Hotkey CoreStation

Criar uma conexão

Você pode criar uma conexão com o Amulet Hotkey CoreStation usando:

- Studio
- Comandos PowerShell

Criar uma conexão usando o Studio

1. Na página **Adicionar Conexão e Recursos**, selecione **Amulet Hotkey CoreStation** como o tipo de conexão.
2. Insira o endereço de conexão do seu Gerenciador de gabinete Amulet Hotkey CoreStation. Você pode usar um endereço IP, nome de host ou FQDN para o endereço.
3. Insira suas credenciais administrativas do gabinete e um nome de conexão amigável.

   A configuração da conexão para quando uma das seguintes situações ocorre:

   - O DaaS recebe um certificado assinado por CA público com erros: Uma mensagem de erro aparece. Siga as instruções na tela para corrigir o problema. Caso contrário, você não poderá prosseguir com a criação da conexão.
   - O DaaS recebe um certificado assinado por CA privado: Uma página de aviso aparece. Compare a impressão digital recebida com a do servidor para verificar a validade do certificado. Se for válido, selecione Confiar no certificado e clique em OK para prosseguir com a criação da conexão. O DaaS então confiará no certificado e armazenará a impressão digital para validação futura.

Criar uma conexão usando comandos PowerShell

Ao criar uma conexão usando o comando PowerShell, forneça as seguintes informações:

- IP: Endereço IP do Amulet Hotkey CoreStation
- Nome de usuário: Nome de usuário do Amulet Hotkey CoreStation
- Senha: Senha do Amulet Hotkey CoreStation

Exemplo:

```
Get-ConfigZone

Get-HypHypervisorPlugin

New-Item `

    -ConnectionType "Custom" `

    -HypervisorAddress $IP `

    -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} `

    -Path @("XDHyp:\Connections\$connectionName") `

    -Persist `

    -PluginId "AmuletHotkeyCoreStationFactory" `

    -Scope @() `

    -SecurePassword $Password `

    -UserName $UserName `

    -ZoneUid $ZoneUid `

    -SslThumbprint $SslThumbprint

New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$HypervisorConnectionID
```

Nota:

O parâmetro `-SslThumbprint` é necessário apenas para certificados privados assinados por CA.

Validação de certificado e impressão digital

Para criar uma conexão bem-sucedida com o Amulet Hotkey CoreStation, o certificado não deve ter erros e a impressão digital deve ter um valor correto. A seguir estão os casos de uso relacionados à validação de certificado e impressão digital:

CENÁRIO	RESULTADO
Certificado público assinado por CA apresenta erros.	A conexão não é criada com sucesso. Consulte os detalhes do erro e resolva o problema.
Certificado público assinado por CA sem erros.	A conexão é criada com sucesso, e o valor `SslThumbprints` é `Null`.
Certificado assinado por CA privada sem erros e um valor `sslthumbprint`.	A conexão é criada com sucesso com um valor `SslThumbprints` correto.
Certificado assinado por CA privada com um valor de impressão digital incorreto.	A conexão não é criada com sucesso.
Certificado assinado por CA privada sem erros. (nenhuma impressão digital fornecida)	A conexão é criada com sucesso. O `SSlThumbprints` é `Null` ao criar a conexão. O valor `SSlThumbprints` é atualizado para um valor pelo serviço do site.

Gerenciar conexões

Corrigir problemas de certificado

O Citrix DaaS bloqueia uma conexão do Amulet Hotkey CoreStation quando surgem problemas de certificado, impedindo que você entregue e gerencie cargas de trabalho em nós associados do Amulet Hotkey CoreStation. Você verá um ícone de erro ao lado da conexão na lista **Conexões de host**.

Consulte a tabela a seguir para problemas e soluções específicas.

PROBLEMA	SOLUÇÃO
Ocorre um erro de certificado para o certificado assinado por CA pública.	Clique na conexão e selecione a guia **Solução de problemas**. Visualize os

PROBLEMA	SOLUÇÃO
	detalhes do erro e resolva o problema.
O certificado recebido é assinado por CA privada ou expirou.	Edite a conexão do host para atualizar a impressão digital do certificado. Etapas detalhadas: 1. Selecione a conexão e clique em **Editar Conexão**. 2. Na página **Propriedades da Conexão**, clique em **Editar configurações**. 3. Insira a senha para se conectar ao gabinete Amulet Hotkey CoreStation e, em seguida, clique em **Salvar**. 4. Na página de **Aviso** que aparece, compare a impressão digital recebida com a do servidor para validar o certificado. 5. Se forem iguais, selecione **Confiar no certificado** e clique em **OK**.

Atualizar valor da impressão digital

Após criar a conexão, você pode atualizar o valor da impressão digital de uma conexão usando o comando PowerShell `Set-Item`. Siga as etapas para atualizar o valor da impressão digital.

1. Obtenha os detalhes de conexão de uma conexão. Por exemplo:

```
Get-Item -LiteralPath xdhyp:\connections\AmuletCon-101
```

2. Atualize o valor do thumbprint. Por exemplo:

```
Set-Item -LiteralPath xdhyp:\connections\AmuletCon-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. Verifique o valor do thumbprint atualizado. Por exemplo:

```
Get-Item -LiteralPath xdhyp:\connections\AmuletCon-101
```

Nota:

A atualização falha se você fornecer um valor de thumbprint incorreto no comando `Set-Item`.

Onde ir a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações sobre o Amulet Hotkey CoreStation, consulte Criar um catálogo de máquinas Amulet Hotkey CoreStation

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização Amulet Hotkey CoreStation

Conexão com AWS EC2

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de nuvem AWS.

Pré-requisitos

Faça o seguinte antes de criar uma conexão com o AWS EC2:

- Conclua a configuração da sua AWS como um local de recurso. Consulte Ambientes de virtualização AWS.
- Defina as permissões do IAM da política de usuário ou função do IAM para que a Citrix gerencie os recursos da AWS em seu nome.

Definir permissões do IAM

Antes de criar uma conexão de host, uma política de permissões do IAM precisa ser definida corretamente para um usuário ou função do IAM que conceda à Citrix as permissões adequadas para provisionar e gerenciar recursos em sua conta AWS em seu nome. Use as informações nesta seção para definir permissões do IAM para o Citrix DaaS na AWS. O serviço IAM da Amazon permite que contas tenham vários usuários, que podem ser organizados em grupos. Esses usuários podem possuir diferentes permissões para controlar sua capacidade de realizar operações associadas à conta. Para obter mais informações sobre permissões do IAM, consulte a referência de política JSON do IAM.

Para aplicar a política de permissões do IAM a um novo grupo de usuários:

1. Faça login no console de gerenciamento da AWS e selecione o **serviço IAM** na lista suspensa.
2. Selecione **Criar um Novo Grupo de Usuários**.
3. Digite um nome para o novo grupo de usuários e selecione **Continuar**.
4. Na página **Permissões**, escolha **Política Personalizada** e, em seguida, **Selecionar**.
5. Digite um nome para a **política de Permissões**.
6. Na seção **Documento de Política**, insira as permissões relevantes.

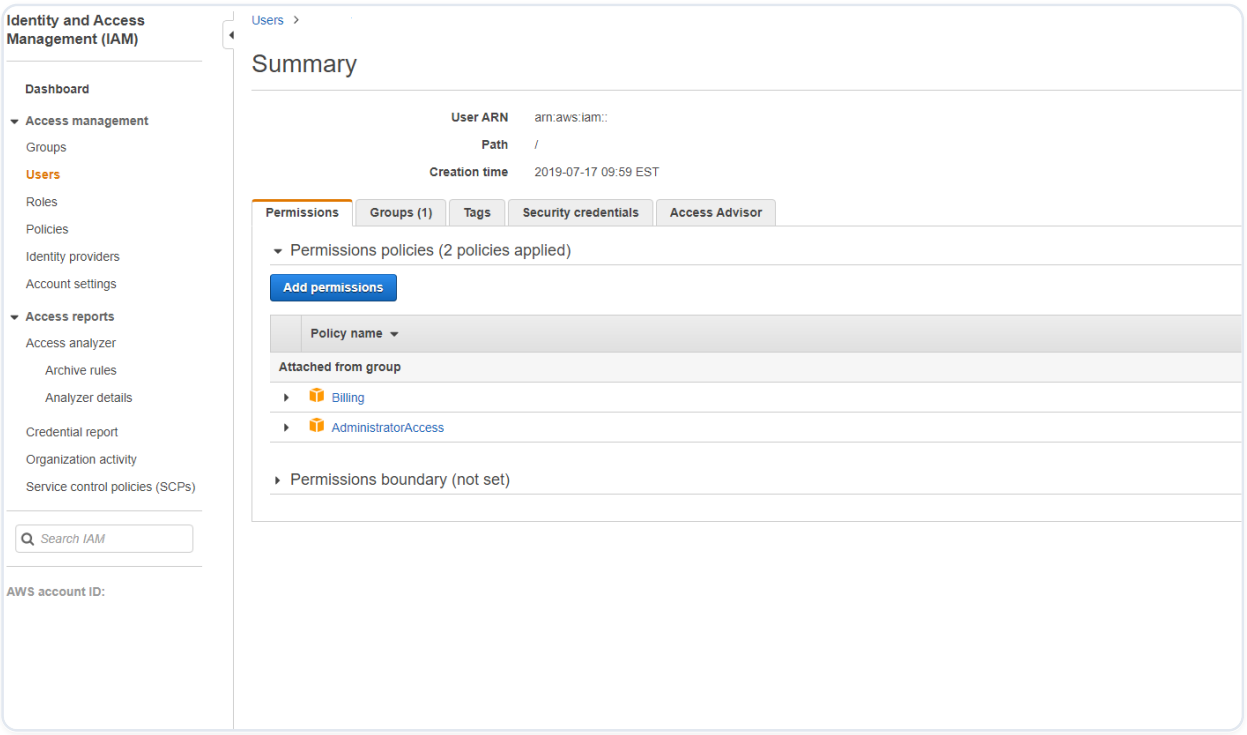
Após inserir as informações da política, selecione **Continuar** para concluir a aplicação da política de permissões IAM ao grupo de usuários. Os usuários do grupo recebem permissões para realizar apenas as ações necessárias para o Citrix DaaS.

> **Importante:**
>
> Use o texto da política fornecido no exemplo deste artigo para listar as ações que um Citrix DaaS usa para executar ações em uma conta AWS sem restringir essas ações a recursos específicos. A Citrix recomenda que você use o exemplo para fins de teste. Para ambientes de produção, você pode optar por adicionar mais restrições aos recursos.

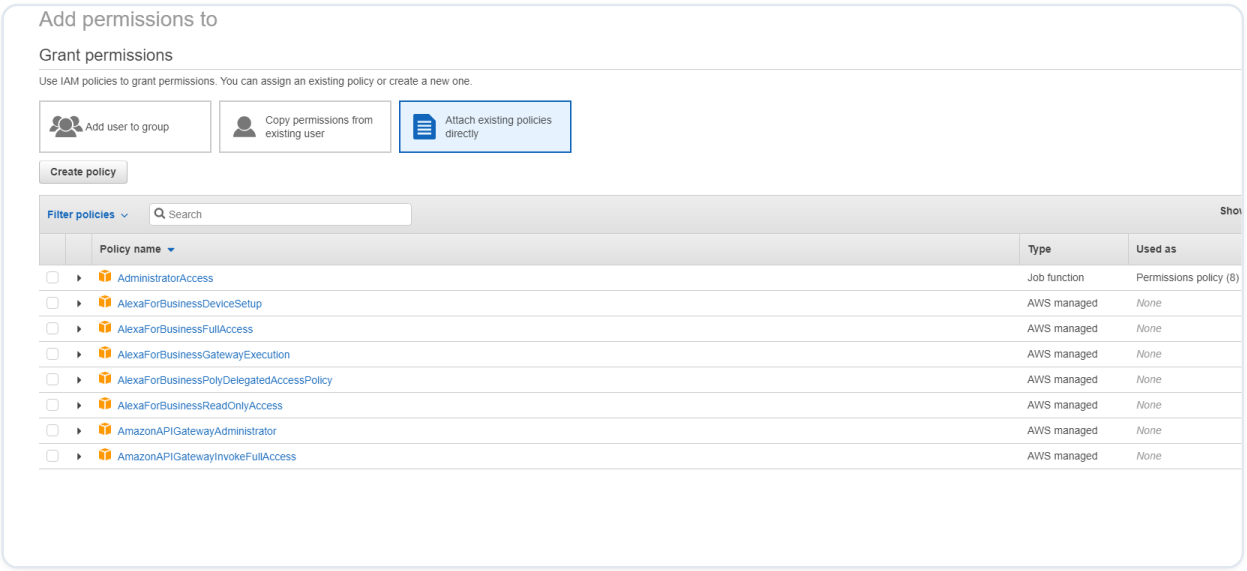
Adicionar permissões IAM

Adicione as permissões na seção **IAM** do AWS Management Console:

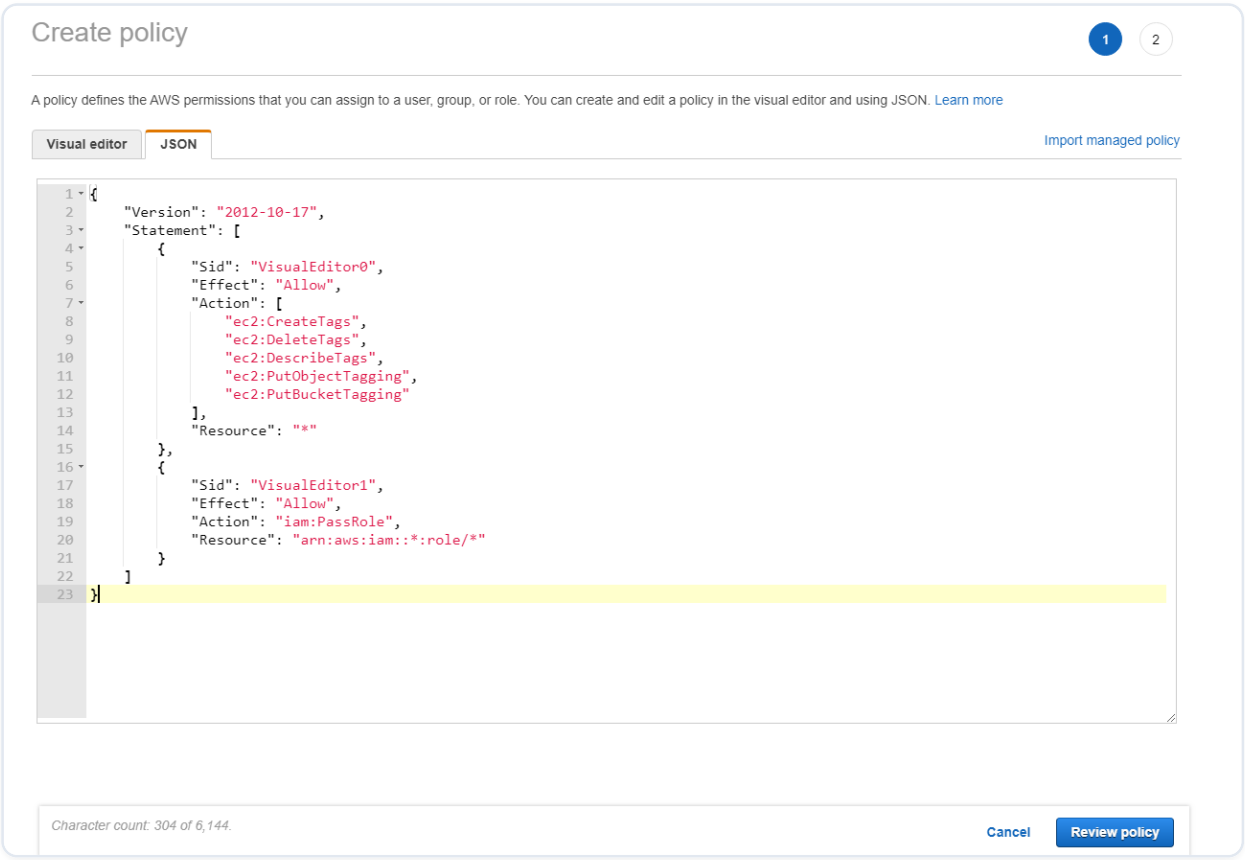
1. No painel **Resumo**, selecione a guia **Permissões**.
2. Selecione **Adicionar permissões.**



3. Na tela **Adicionar Permissões a**, conceda permissões:



4. Na seção JSON, inclua Permissões AWS necessárias para o seu ambiente.



Criar uma conexão

Você pode criar uma conexão com o Amazon EC2 usando:

- Studio
- Comandos PowerShell

> **Nota:**

> Verifique as restrições do seu servidor proxy ou firewall e certifique-se de que o seguinte endereço seja contatável: `https://*.amazonaws.com`. Além disso, certifique-se de que todos os endereços mencionados em conectividade do serviço Citrix Gateway sejam contatáveis.

> Se estes não forem contatáveis, isso pode causar falha ao criar ou atualizar a conexão do host.

Criar uma conexão usando o Studio

1. navegar para a página **Hosting > Add Connection and Resources**.

2. Na página **Connection**, siga estas etapas para configurar a conexão:

    a. Selecione **Criar uma nova conexão**.

    b. Em **Zone**, selecione o local do recurso que você configurou para seu ambiente AWS.

    c. Selecione **Amazon EC2** como o tipo de conexão.

    d. Selecione um dos métodos para provisionar os recursos:

    - Se você selecionar **Usar esta conta AWS para provisionar recursos**, selecione **Usar chave de acesso de usuário IAM** ou **Usar função IAM**. Para a chave de acesso de usuário IAM, forneça sua **chave de API** e **chave secreta** para o usuário IAM que possui a política de permissões IAM adequada para a Citrix gerenciar recursos em sua conta AWS. Para a função IAM, certifique-se de ter atribuído uma função IAM à instância do Citrix Cloud Connector com a política de permissões IAM adequada para a Citrix gerenciar recursos em sua conta AWS. Consulte Guia de autenticação baseada em função para obter mais informações.
    - Se você selecionar **Usar acesso entre contas para provisionar recursos**, forneça o **ARN** da função IAM na Conta B que os Cloud Connectors (ou Delivery Controllers) na Conta A devem assumir e executar operações de provisionamento.

    e. Insira um nome de conexão e clique em **Avançar**.

3. Na página **Local da Máquina Virtual**, especifique o local onde as VMs devem ser provisionadas. Selecione a região da nuvem, VPC e zona de disponibilidade ou zona local para criar novas VMs.
4. Na página **Rede**:

    a. Insira um nome para os recursos que você selecionou anteriormente na zona de disponibilidade ou zona local.

    b. Selecione uma ou mais sub-redes na VPC que você configurou no menu anterior.

5. Clique nas páginas restantes até a página **Resumo**.
6. Clique em **Concluir** para criar a conexão de host com o Amazon EC2.

CONSIDERAÇÕES IMPORTANTES

Ao criar uma conexão usando o Studio:

- Defina as permissões IAM adequadas para que a Citrix gerencie seus recursos AWS.
- Se você usar uma chave de acesso de usuário IAM para a Citrix gerenciar seus recursos AWS, deverá fornecer os valores da chave de API e da chave secreta. Você pode exportar o

arquivo de chave contendo esses valores do AWS e depois importá-los. Você também deve fornecer a região, zona de disponibilidade, nome da VPC, endereços de sub-rede, nome de domínio, nomes de grupos de segurança e credenciais.

- Se você usar uma função IAM para a Citrix gerenciar seus recursos AWS, deve-se certificar de atribuir uma função com as permissões IAM adequadas a todos os seus Cloud Connector(s). Guia de autenticação baseada em função para obter mais informações.
- O arquivo de credenciais para a conta raiz do AWS (recuperado do console do AWS) não é formatado da mesma forma que os arquivos de credenciais baixados para usuários padrão do AWS. Portanto, o Citrix DaaS não pode usar o arquivo para preencher os campos de chave de API e chave secreta. Certifique-se de que você está usando arquivos de credenciais do AWS Identity Access Management (IAM).
- A zona pode ser uma zona de disponibilidade ou zona local.

Criar uma conexão usando o PowerShell

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute os seguintes comandos. A seguir, um exemplo:

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$apiSecret = “bbbbb”

$secureKey = ConvertTo-SecureString -String $apiSecret

$zoneUid = "00000000-0000-0000-0000-000000000000"

$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath -ConnectionType "<name of
the connection>" -HypervisorAddress " "@("https://ec2.cn-
north-1.amazonaws.com.cn") -Persist -Scope @() -UserName $apiKey
-SecurePassword $secureKey -ZoneUid $zoneUid
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid



$hostingUnitName = "demo-hostingunit"

$availabilityzone = "us-east-1a"

$vpcName = "Default VPC"

$jobGroup = [Guid]::NewGuid()

$hostingUnitPath = "XDHyp:\HostingUnits\" + $HostingUnitName

$rootPath = $connectionPath + "\" + $vpcName + ".virtualprivatecloud\"

$availabilityZonePath = @($rootPath + $availabilityzone +
".availabilityzone")

$networkPaths = (Get-ChildItem $availabilityZonePath[0] | Where
ObjectType -eq "Network") | Select-Object -ExpandProperty FullPath #
will select all the networks in the availability zone



New-Item -Path $hostingUnitPath -AvailabilityZonePath
$availabilityZonePath -HypervisorConnectionName $connectionName
-JobGroup $jobGroup -PersonalvDiskStoragePath @() -RootPath $rootPath
-NetworkPath $networkPaths
```

Nota:

Para criar uma conexão usando a Autenticação Baseada em Função, especifique apiKey e apiSecret como `role_based_auth`.

Limitação

Se você alterar o nome de uma Nuvem Privada Virtual (VPC) da AWS no console da AWS, a unidade de hospedagem existente no Citrix Cloud™ será quebrada. Quando a unidade de hospedagem está quebrada, você não pode criar catálogos ou adicionar máquinas a catálogos existentes. Para resolver o problema, altere o nome da VPC da AWS de volta para o nome original.

Configuração de proxy aprimorada para conexão de host AWS

A conexão de host AWS pode ler o valor do proxy do sistema WinHTTP que é configurado durante a instalação do Cloud Connector se você definir a propriedade personalizada `UseSystemProxyForHypervisorTrafficOnConnectors` como `true` ao criar ou atualizar uma conexão de host usando o PowerShell.

Vantagens

- Simplifica a configuração de proxy para conexões de host AWS.
- Reduz a necessidade de configuração manual de valores de servidor e porta via PowerShell.
- Garante o uso consistente de proxy entre o Cloud Connector e as conexões de host.
- Melhora a taxa de sucesso das chamadas de API que exigem acesso via proxy.
- Diminui as solicitações de suporte relacionadas à configuração de proxy.

Pré-requisito

Antes de definir a propriedade personalizada ao criar a conexão de host usando o PowerShell, certifique-se de configurar o proxy WinHTTP no Cloud Connector.

Criar uma nova conexão com proxy automático

1. Abra o PowerShell.
2. Adicione os snap-ins do Citrix:

```
Add-PSSnapin citrix*
```

3. Defina as variáveis para a conexão.

```
$hypType = "AWS"



##############################################################################
```

```
#############

The following items need to be set based on the installed environment

$customProperties is set to enable using the system proxy

$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" /></
CustomProperties>'



$awsEndPoint is set to the desired region for the connection



$awsEndPoint = "https://ec2.us-east-1.amazonaws.com"



$hypConnName is set to the connection name to use



$hypConnName = "ctx-test"



$apiKey is set to the AWS API Key ID or "role_based_auth" if the Cloud
Connector instance has an appropriate role



$apiKey = "role_based_auth"



$secretKey is set to the AWS API Key Secret or "role_based_auth" if the
Cloud Connector instance has an appropriate role
```

```
$secretKey = "role_based_auth"



$resourceLocation is set to the connector resource location name



$resourceLocation = "ctx-test"

##############################################################################
#############



$secureSecretKey = ConvertTo-SecureString -String $secretKey
-AsPlainText -Force

$zoneUid = (Get-ConfigZone|Where-Object Name -EQ
"$resourceLocation").Uid
```

Nota:

Certifique-se de substituir os valores de espaço reservado nas variáveis `$customProperties`, `$awsEndPoint`, `$hypConnName`, `$apiKey`, `$secretKey` e `$resourceLocation` pelos valores apropriados para o seu ambiente.

4. Crie a conexão do hipervisor.

```
$hypHc = New-Item -Path xdhyp:\Connections `

-Name $hypConnName `

-HypervisorAddress $awsEndPoint `

-UserName $apiKey `

-SecurePassword $secureSecretKey `
```

```
-ConnectionType $hypType `

-CustomProperties $customProperties `

-Persist `

-ZoneUid $zoneUid
```

5. Crie a conexão do hipervisor do Broker.

```
$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid
```

Consulte também Atualizar uma conexão de host existente com proxy automático

Provisionamento entre contas

Existem casos de uso em que os Cloud Connectors gostariam de ser colocados em uma conta AWS separada (conta de serviços compartilhados ou conta de componentes de site) com funções IAM que têm acesso entre contas (função IAM entre contas) e catálogos de máquinas provisionados por MCS em uma conta AWS secundária separada (contas de cargas de trabalho), sem a necessidade de Cloud Connectors adicionais nas contas separadas. Para suportar tais cenários, este recurso usa o emparelhamento de VPC e o acesso entre contas usando funções IAM para tornar o provisionamento entre diferentes contas AWS possível para empresas que gerenciam várias contas AWS.

Com emparelhamento de VPC, você pode fazer com que seu Cloud Connector e VMs provisionadas em diferentes regiões ou contas possam se comunicar entre si.

Com acesso entre contas usando funções IAM, você permite que a conta primária (conta do Cloud Connector) assuma uma função IAM para acessar recursos AWS na conta secundária (VMs do catálogo de máquinas).

Para permitir que o Cloud Connector acesse os recursos da conta secundária, crie uma conexão de host após assumir a função IAM da conta secundária.

Pré-requisitos

Configure o seguinte antes de criar uma conexão de host para provisionamento entre contas:

- Configure o emparelhamento de VPC e os grupos de segurança em ambas as regiões ou contas. Consulte Configurar emparelhamento de VPC.
- Delegue o acesso entre contas usando funções IAM. Consulte Delegar acesso entre contas usando a função IAM.

Configurar emparelhamento de VPC

Vamos supor que a VPC A esteja na conta principal (Conta A) e tenha os Cloud Connectors e o Active Directory. A VPC B está na conta secundária (Conta B) onde você deseja provisionar as VMs.

Para configurar uma conexão de emparelhamento de VPC entre a Conta A e a Conta B, faça o seguinte:

1. Crie uma conexão de emparelhamento de VPC. Consulte:
   - Conta diferente, mesma região
   - Conta diferente, região diferente
2. Vá para sua VPC A e para a tabela de rotas associada à sub-rede pública.
3. Clique em **Editar Rotas > Adicionar rota**. Adicione o bloco CIDR da VPC B na coluna **Destino** e adicione o emparelhamento de VPC que você criou na coluna **Alvo**.
4. Repita as Etapas 2 e 3, mas com as sub-redes privadas para VPC A e VPC B (adicione o bloco CIDR da VPC A). Consulte Atualizar suas tabelas de rotas para uma conexão de emparelhamento de VPC.
5. Vá para o grupo de segurança privado associado à VPC A.
6. Selecione **Ações** e, em seguida, **Editar regras de entrada**.
7. Selecione **Adicionar regra**. Para tipo, selecione **Todo o Tráfego** e, em seguida, na **Coluna de Origem** adicione:
   - Se for uma região diferente, adicione o Bloco CIDR da VPC B.
   - Se for uma conta diferente, mas na mesma região, adicione o ID da conta e o ID do grupo de segurança privado da VPC B, separados por uma barra (Exemplo: 123456789012/sg-1a2b3c4d)
8. Repita os Passos 5 a 7, mas com o grupo de segurança privado para a VPC B (mas adicione o Bloco CIDR da VPC A ou o ID da conta da VPC A e o ID do grupo de segurança privado da mesma região, mas de uma conta diferente). Consulte Atualize seus grupos de segurança para referenciar grupos de segurança pares.

> **Nota:**
>
> Não há cobrança para criar uma conexão de emparelhamento de VPC. No entanto, embora o emparelhamento de VPC dentro de uma Zona de Disponibilidade seja gratuito, aplicam-se cobranças quando a transferência de dados por uma conexão de emparelhamento de VPC ocorre em várias Zonas de Disponibilidade e regiões. Consulte Preços para uma conexão de emparelhamento de VPC.

Delegar acesso entre contas usando funções IAM

Após configurar o emparelhamento de VPC entre contas, você delega o acesso entre contas usando funções IAM.

Com o acesso entre contas usando funções IAM, você permite que a conta primária (conta do Cloud Connector) assuma uma função IAM para acessar recursos AWS na conta secundária (VMs do catálogo de máquinas).

Para acessar recursos entre contas, faça o seguinte:

> **Lembre-se:**
>
> Assumindo que a VPC A está na conta primária (Conta A) e possui o Cloud Connector e o Active Directory. A VPC B está na conta secundária (Conta B) onde você deseja provisionar as VMs

1. Configure o emparelhamento de VPC entre contas com as etapas mencionadas anteriormente.
2. Crie uma função e política IAM na Conta B com permissões IAM mínimas da Citrix. Consulte Tutorial IAM: Delegar acesso entre contas AWS usando funções IAM. Digamos que o ARN desta função seja "arn:aws:iam::5678:role/citrix-role".
3. Adicione a política de Confiança à função "arn:aws:iam::5678:role/citrix-role" para que ela possa ser acessada pela função da Conta A "arn:aws:iam::1234:role/primary-account-citrix-role", conforme - Acesso a recursos entre contas no IAM.
4. Crie a função e política IAM na Conta A com o nome mencionado anteriormente "primary-account-citrix role”, que pode assumir a função IAM e passar a função IAM da Conta B (arn:aws:iam::5678:role/citrix-role).

5. Atribua a função "arn:aws:iam::1234:role/primary-account-citrix-role" a todos os Cloud Connectors na Conta A.

Os Cloud Connectors agora podem assumir a função da Conta B ("arn:aws:iam::5678:role/citrix-role").

Criar conexão de host para provisionamento entre contas

Crie uma conexão de host na conta secundária (Conta B) onde você deseja provisionar as VMs. Isso permite que os Cloud Connectors da Conta A acessem os recursos na Conta B após assumir a função da Conta B.

Use comandos PowerShell para criar a conexão de host e adicionar as duas propriedades personalizadas a seguir:

- `CrossAccountRoleArn`: Se você não fornecer a propriedade `CrossAccountRoleArn`, a Conexão de Host regular será criada. Neste caso, `MaximumAssumeRoleDurationInSeconds` é ignorado mesmo que seja fornecido.
- `MaximumAssumeRoleDurationInSeconds`: `DurationInSeconds` deve estar entre 900 segundos e 3600 segundos. O padrão é 900 segundos. Se você fornecer um valor maior que 3600, então `DurationInSeconds` será definido como 3600.

Exemplo:

```
$connectionName = "cross-account-conn"

$cloudRegion = "us-east-1"

$apiKey = "role_based_auth"

$secretKey = "role_based_auth"

$zoneUid = "xxxxxx"

$secureKey = (ConvertTo-SecureString -String $secretKey -AsPlainText
-Force)

$connectionPath = "XDHyp:\Connections\" + $connectionName

$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```
<Property xsi:type="StringProperty" Name="CrossAccountRoleArn"
Value="arn:aws:iam::5678:role/citrix-role" /><Property
xsi:type="StringProperty" Name="MaximumAssumeRoleDurationInSeconds"
Value="3600" />

"</CustomProperties>'



$connection = New-Item -Path $connectionPath -ConnectionType "AWS"
-HypervisorAddress "https://ec2.$($cloudRegion).amazonaws.com" -Persist
-Scope @() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
-CustomProperties $customProperties



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

Após a criação da conexão de host, crie unidades de hospedagem usando o Studio ou PowerShell. No entanto, selecione VPC e Redes.

Editar uma conexão

Você pode editar uma conexão de host existente para:

- Modificar a opção para fornecer permissões IAM para a Citrix gerenciar recursos
- Modificar o número máximo de ações simultâneas (ou máquinas concorrentes) por conexão de hospedagem
- Modificar o escopo.
- Configurar o número máximo de grupos de segurança permitidos por interface de rede elástica (ENI) usando o comando PowerShell
- Atualizar uma conexão de host existente com proxy automático

Editar opções para fornecer permissões IAM

1. Clique com o botão direito do mouse em uma conexão Amazon EC2 existente.
2. Na página **Propriedades da Conexão**, clique em **Editar configurações**.
3. Selecione uma das opções para fornecer permissões IAM para a Citrix gerenciar recursos. Insira os detalhes necessários e clique em **Salvar**.

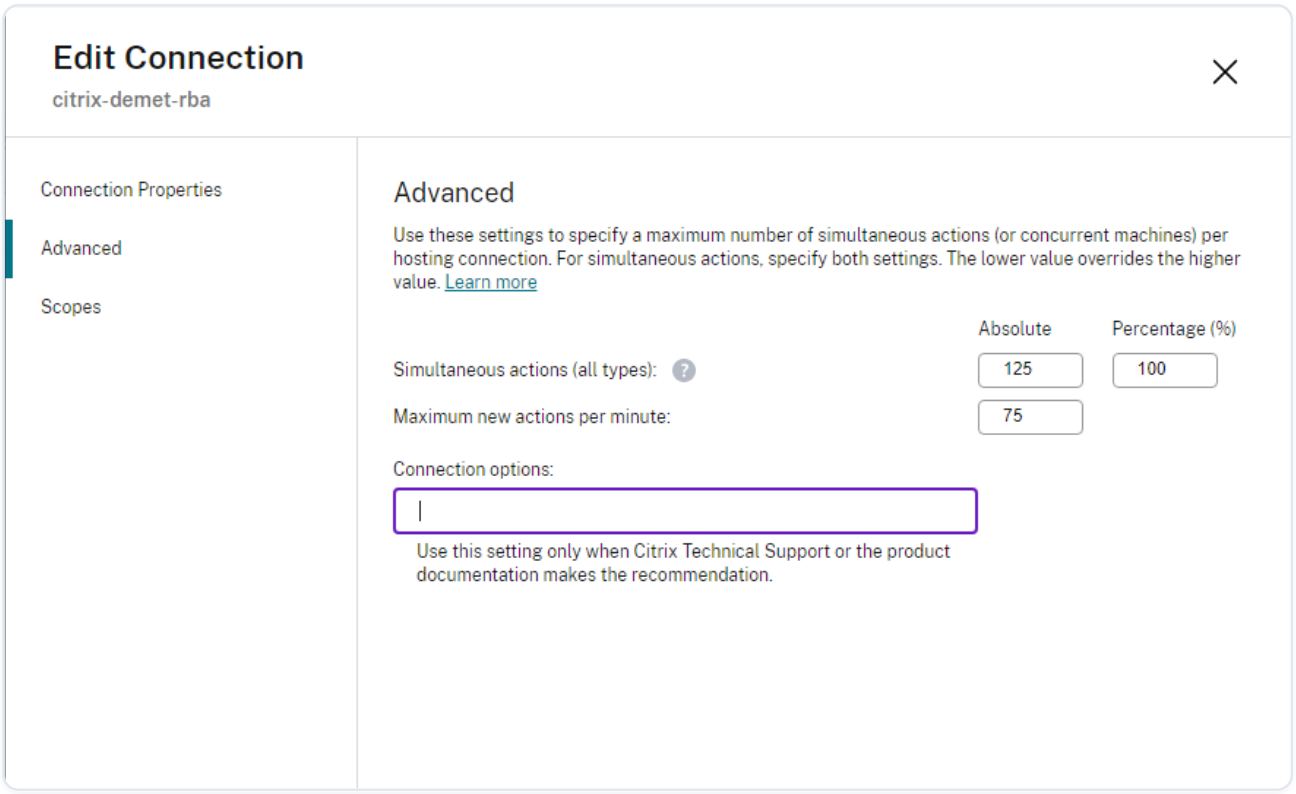
Modificar o número máximo de ações simultâneas

Ao criar conexões de host no Studio para Amazon EC2, os seguintes valores padrão são exibidos:

OPÇÃO	ABSOLUTO	PORCENTAGEM
Ações simultâneas (todos os tipos)	125	100
Máximo de novas ações por minuto	150	n/d
Número máximo de operações de provisionamento simultâneas	100	n/d

O MCS suporta 100 operações de provisionamento simultâneas máximas por padrão.

Configure esses valores acessando a seção **Avançado** do Citrix Studio na tela **Editar Conexão**.



Alternativamente, você pode usar o SDK do PowerShell Remoto para definir o número máximo de operações simultâneas para configurações ideais por ambiente.

Use a propriedade personalizada do PowerShell, `MaximumConcurrentProvisioningOperations`, para especificar o número máximo de operações de provisionamento simultâneas da AWS.

Antes da configuração:

- Certifique-se de ter instalado o SDK do PowerShell para a Nuvem.
- Entenda que o valor padrão para `MaximumConcurrentProvisioningOperations` é 100.

Execute as seguintes etapas para personalizar o valor `MaximumConcurrentProvisioningOperations`:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Insira `cd xdhyp:\Connections\`.
4. Insira `dir` para listar as conexões.
5. Altere ou Inicialize a string de Propriedades Personalizadas:
   - Se a string de Propriedades Personalizadas tiver um valor, copie as Propriedades Personalizadas para o Bloco de Notas. Em seguida, altere a propriedade `MaximumConcurrentProvisioningOperations` para o valor de sua preferência. Você pode inserir um valor no intervalo de 1 a 1000. Por exemplo, `<Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`.
   - Se a string de Propriedades Personalizadas estiver vazia ou nula, você deve inicializar a string inserindo a sintaxe apropriada tanto para o esquema quanto para a propriedade `MaximumConcurrentProvisioningOperations`.
6. Na janela do **PowerShell**, cole as Propriedades Personalizadas modificadas do Bloco de Notas e atribua uma variável às Propriedades Personalizadas modificadas. Se você inicializou as Propriedades Personalizadas, adicione as seguintes linhas após a sintaxe:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="100"/></CustomProperties>'
   ```

   Esta string define a propriedade `MaximumConcurrentProvisioningOperations` como 100. Na string de Propriedades Personalizadas, você deve definir a propriedade `MaximumConcurrentProvisioningOperations` para um valor que se alinhe às suas necessidades.

7. Insira `Get-XDAuthentication`, que solicitará suas credenciais.
8. Execute `$cred = Get-Credential`, que pode solicitar apenas uma Senha (ou um Nome e Senha). Você também pode ser solicitado a fornecer o ID do aplicativo e o segredo associado. Para conexões que usam autenticação baseada em função, **role_based_auth** é tanto o Nome quanto a Senha. Caso contrário, insira o ID da API AWS e o segredo.
9. Execute `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`. Você deve definir *<connection-name>* para o nome da conexão.
10. Insira `dir` para verificar a string CustomProperties atualizada.

Configurar grupos de segurança por interface de rede

Ao editar uma conexão de host, agora você pode configurar o número máximo de grupos de segurança permitidos por interface de rede elástica (ENI) usando um comando PowerShell. Para obter informações sobre os valores de cota de grupos de segurança da AWS, consulte Grupos de segurança.

Para configurar grupos de segurança por interface de rede:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute `cd xdhyp:\Connections\`.
4. Execute `dir` para listar as conexões.
5. Execute o seguinte comando PowerShell para configurar grupos de segurança por interface de rede:

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws -Name
"Citrix_MachineManagement_Options" -Value "
AwsMaxENISecurityGroupLimit=<number>"
```

> **Nota:**
>
> Se você não definir um valor para `AwsMaxENISecurityGroupLimit`, ele assumirá o valor padrão de 5.

Atualizar uma conexão de host existente com proxy automático

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Insira `cd xdhyp:\Connections\`.
4. Insira `dir` para listar as conexões.
5. Copie as CustomProperties para um bloco de notas e anexe a configuração de propriedade `<Property xsi:type="StringProperty" Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True"`.
6. Na janela do **PowerShell**, cole as Custom Properties modificadas do Bloco de Notas e atribua uma variável às Custom Properties modificadas.
7. Insira `Get-XDAuthentication`, que solicitará suas credenciais.
8. Execute `$cred = Get-Credential`, que pode solicitar apenas uma Senha (ou um Nome e Senha). Você também pode ser solicitado a fornecer o ID do aplicativo e o segredo associado. Para conexões que usam autenticação baseada em função, **role_based_auth** é o Nome e a Senha. Caso contrário, insira o ID e o segredo da API AWS.
9. Execute `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`. Você deve definir \<*connection-name*\> como o nome da conexão.
10. Insira `dir` para verificar a string CustomProperties atualizada.

URL do endpoint de serviço

URL do endpoint de serviço da zona padrão

Ao usar o MCS, uma nova conexão AWS é adicionada com uma chave de API e um segredo de API. Com essas informações, juntamente com a conta autenticada, o MCS consulta a AWS para as zonas suportadas usando a chamada de API AWS DescribeRegions EC2. A consulta é feita usando uma URL de endpoint de serviço EC2 genérica `https://ec2.amazonaws.com/`. Use o MCS para selecionar a zona para a conexão na lista de zonas suportadas. A URL de endpoint de serviço AWS preferencial é selecionada automaticamente para a zona. No entanto, depois de criar a URL do endpoint de serviço, você não pode mais definir ou modificar a URL.

URL de endpoint de serviço não padrão

Pode haver situações em que você não precise da URL de endpoint de serviço AWS escolhida automaticamente para a conexão. Nesses casos, você pode usar o Citrix Cloud SDK e o PowerShell para criar uma conexão com uma URL de endpoint de serviço não padrão. Por

exemplo, para criar uma conexão usando a URL do endpoint de serviço `https://ec2.cn-north-1.amazonaws.com.cn`:

1. Configure o Cloud Connector hospedado na AWS e certifique-se de que ele tenha conectividade.
2. Execute os seguintes comandos do PowerShell para ver a lista de Cloud Connectors.

```
PS C:\> asnp citrix.*

PS C:\> Get-XDAuthentication

PS C:\> Get-ConfigEdgeServer
```

3. Encontre o ZoneUid do Cloud Connector recém-criado e insira-o nos seguintes comandos do PowerShell. Substitua os itens em itálico pelos respectivos valores.

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUid`*ZoneUid*`-
Name`*"My New Connection”*`-ConnectionType "AWS" -HypervisorAddress
@("https://ec2.cn-north-1.amazonaws.com.cn") -UserName`*"APIkey"* `-
Password`*“API Secret”* `-Persist`

`PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hyp. HypervisorConnectionUid
```

4. Atualize a guia **Hospedagem** para verificar se a conexão EC2 foi criada.
5. Adicione um local de recurso usando a nova conexão.

Permissões AWS necessárias

Esta seção contém a lista completa de permissões AWS. Use o conjunto completo de permissões conforme fornecido na seção para que a funcionalidade funcione corretamente.

> **Nota:**
>
> A permissão `iam:PassRole` é necessária apenas para **role_based_auth**.

Criando uma conexão de host

Uma nova conexão de host é adicionada usando as informações obtidas da AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Gerenciamento de energia de VMs

As VMs são ligadas ou desligadas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
```

```
                "ec2:DescribeInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "ec2:DescribeInstanceStatus"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Criando, atualizando ou excluindo VMs

Um catálogo de máquinas é criado, atualizado ou excluído com VMs provisionadas como instâncias AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
```

```
                "ec2:RevokeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateSecurityGroup",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",


                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Nota:

- A seção EC2 relacionada a SecurityGroups é necessária apenas se um Grupo de Segurança de Isolamento precisar ser criado para a VM de Preparação durante a criação do catálogo. Uma vez feito isso, essas permissões não são mais necessárias.

Importando VMs

Um catálogo de máquinas é criado importando VMs.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeInstances",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeSubnets",

                "ec2:DescribeVolumes",

                "ec2:DescribeSpotInstanceRequests"

            ],

            "Effect": "Allow",

            "Resource": "*"

        }

    ]

}
```

Nota:

O `ec2:DescribeSpotInstanceRequests` é necessário apenas se houver uma instância spot na região AWS de onde as VMs serão importadas.

UPLOAD E DOWNLOAD DIRETO DE DISCO

O upload direto de disco elimina o requisito de volume worker para provisionamento de catálogo de máquinas e, em vez disso, usa APIs públicas fornecidas pela AWS. Essa funcionalidade reduz o custo associado a contas de armazenamento extras e a complexidade de manter as operações de volume worker.

Nota:

O suporte para volume worker foi removido. As permissões de upload e download direto de disco são necessárias para o provisionamento de catálogo de máquinas.

As seguintes permissões devem ser adicionadas à política:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

Importante:

- Você pode adicionar uma nova VM a catálogos de máquinas existentes sem quaisquer recursos de volume worker, como AMI de volume worker e VM de volume worker.

- Se você excluir um catálogo existente que usou qualquer volume worker antes, todos os artefatos relacionados ao volume worker serão excluídos.

Criptografia EBS de volumes criados

O EBS pode criptografar automaticamente volumes recém-criados se a AMI for criptografada, ou se o EBS estiver configurado para criptografar todos os novos volumes. No entanto, para implementar a funcionalidade, as seguintes permissões devem ser incluídas na política do IAM.

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Nota:

As permissões podem ser limitadas a chaves específicas, incluindo um bloco de Recurso e Condição a critério do usuário. Por exemplo, **Permissões KMS com Condição**:

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
```

```
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

A seguinte declaração de política de chave é a política de chave padrão completa para chaves KMS que é necessária para permitir que a conta use políticas do IAM para delegar permissão para todas as ações (kms:*) na chave KMS.

```
{
"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::111122223333:root"
},
"Action": "kms:",
"Resource": ""
}
```

Para obter mais informações, consulte a documentação oficial do AWS Key Management Service.

Autenticação baseada em função do IAM

As seguintes permissões são adicionadas para suportar a autenticação baseada em função.

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

Política de permissões mínimas do IAM

O JSON a seguir pode ser usado para todos os recursos atualmente suportados. Você pode criar conexões de host, criar, atualizar ou excluir VMs e fazer gerenciamento de energia usando esta política. A política pode ser aplicada aos usuários conforme explicado nas seções Definindo permissões do IAM ou você também pode usar a autenticação baseada em função usando a chave de segurança **role_based_auth** e a chave secreta.

Importante:

Para usar **role_based_auth**, primeiro configure a função IAM desejada na instância EC2 do conector de nuvem ao configurar o conector de nuvem. Usando o Citrix Studio, adicione a conexão de hospedagem e forneça o role_based_auth para a chave de autenticação e o segredo. Uma conexão de hospedagem com essas configurações usa então a autenticação baseada em função.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
```

```
                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",
```

```
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
```

```
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
    ]
}
```

Nota:

- A seção EC2 relacionada a SecurityGroups só é necessária se um Grupo de Segurança de Isolamento precisar ser criado para a VM de Preparação durante a criação do catálogo. Uma vez feito isso, essas permissões não são mais necessárias.
- A seção KMS é necessária apenas ao usar a criptografia de volume EBS.
- A seção de permissão `iam:PassRole` é necessária apenas para **role_based_auth**.
- Permissões específicas em nível de recurso podem ser adicionadas em vez de acesso total, com base em seus requisitos e ambiente. Consulte os documentos da AWS Demystifying EC2 Resource-Level Permissions e Access management for AWS resources para obter mais detalhes.
- Use as permissões `ec2:CreateNetworkInterface` e `ec2:DeleteNetworkInterface` somente se estiver usando o método de worker de volume.

Validar permissões na conexão do host

Você pode validar as permissões em uma conexão de host para realizar tarefas relacionadas à criação e gerenciamento de catálogos de máquinas MCS. Essa implementação ajuda você a descobrir as permissões ausentes necessárias para diferentes cenários, como criação, exclusão e

atualização de VMs, gerenciamento de energia de VMs e criptografia EBS, com antecedência, para que você possa evitar ser bloqueado em momentos críticos.

Você pode validar as permissões em uma conexão de host usando o comando PowerShell `Test-HypHypervisorConnection`. O resultado do comando é capturado como uma lista, onde cada item da lista é dividido em três seções.

- Categoria: A ação ou tarefa que um usuário pode realizar para criar e gerenciar um catálogo de máquinas MCS.
- Ação Corretiva: A etapa que um administrador deve realizar para resolver uma discrepância de permissões ausentes dos usuários.
- Permissão ausente: A lista de permissões ausentes para uma categoria.

Para validar as permissões, faça o seguinte:

1. Crie uma conexão de host com a AWS.
2. Abra uma janela do PowerShell no host do Delivery Controller™.
3. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
4. Execute o seguinte comando para verificar se você tem as permissões necessárias para consultar suas permissões.

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AWSCon"
   ```

5. Depois de adicionar as permissões ausentes necessárias para consultar suas permissões, execute o seguinte comando para verificar se você tem permissões nas seguintes categorias:

   - Criar Atualizar excluir
   - Gerenciamento de Energia
   - Criptografia EBS

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:
   \Connections\AWSCon" [-SecurePassword -Password] "password" -UserName
   "" -CustomProperties ""
   ```

Para obter mais informações sobre como adicionar permissões, consulte Adicionar permissões IAM.

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas do AWS, consulte Criar um catálogo AWS EC2.

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização AWS

Conexão com instâncias gerenciadas do Amazon WorkSpaces Core

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos das instâncias gerenciadas do Amazon WorkSpaces Core.

Pré-requisitos

Faça o seguinte antes de criar uma conexão com instâncias gerenciadas do Amazon WorkSpaces Core:

- Conclua a configuração da sua AWS como um local de recurso. Consulte Ambientes de virtualização da AWS.
- Defina as permissões do IAM da política de usuário ou função do IAM para que a Citrix® gerencie os recursos da AWS em seu nome.
- Crie uma função vinculada ao serviço.

Definir permissões do IAM

Antes de criar uma conexão de host, uma política de permissões do IAM precisa ser definida corretamente para um usuário ou função do IAM que conceda à Citrix as permissões adequadas para provisionar e gerenciar recursos em sua conta AWS em seu nome. Use as informações nesta seção para definir permissões do IAM para o Citrix DaaS em instâncias gerenciadas do Amazon WorkSpaces Core. O serviço IAM da Amazon permite contas com vários usuários, que podem ser organizados em grupos. Esses usuários podem possuir diferentes permissões para controlar sua capacidade de realizar operações associadas à conta. Para obter mais informações sobre permissões do IAM, consulte a referência de política JSON do IAM.

> **Nota:**

> Como a Citrix provisiona e gerencia recursos e automação em sua conta AWS em seu nome, a configuração de políticas de permissões do IAM com base em tags específicas ou convenções de nomenclatura de recursos não é suportada.

> Para aplicar a política de permissões do IAM a um novo grupo de usuários:

1. Faça login no console de gerenciamento da AWS e selecione o **serviço IAM** na lista suspensa.
2. Selecione **Criar um Novo Grupo de Usuários**.
3. Digite um nome para o novo grupo de usuários e selecione **Continuar**.
4. Na página **Permissões**, escolha **Política Personalizada**.
5. Digite um nome para a **Política de permissões**.
6. Na seção **Documento de Política**, insira as permissões relevantes.

Após inserir as informações da política, selecione **Continuar** para concluir a aplicação da política de permissões do IAM ao grupo de usuários. Os usuários do grupo recebem permissões para realizar apenas as ações necessárias para o Citrix DaaS.

> **Importante:**

> Use o texto da política fornecido no exemplo deste artigo para listar as ações que um Citrix DaaS usa para executar ações em uma conta AWS sem restringir essas ações a recursos específicos. A Citrix recomenda que você use o exemplo para fins de teste. Para ambientes de produção, você pode optar por adicionar mais restrições aos recursos.

Adicionar permissões IAM

Adicione as permissões na seção **IAM** do AWS Management Console:

1. No painel **Resumo**, selecione a guia **Permissões**.
2. Selecione **Adicionar permissões.**
3. Na tela **Adicionar permissões a**, conceda as permissões.
4. Na seção JSON, inclua Permissões AWS necessárias para o seu ambiente.

Criar uma função vinculada ao serviço

Para cada uma das suas contas AWS das quais o Citrix chamará as APIs Core V2, crie uma função vinculada ao serviço (SLR).

As etapas para criar a função:

- Abra uma Interface de Linha de Comando (CLI) no console de gerenciamento da AWS.
- Execute o seguinte comando na CLI:

```
aws iam create-service-linked-role --aws-service-name workspaces-instances.amazonaws.com
```

Você também pode configurar a função vinculada ao serviço usando o console de gerenciamento do Amazon WorkSpaces Core. Consulte Criação de uma função vinculada ao serviço (console).

Criar uma conexão

Você pode criar uma conexão com instâncias gerenciadas do Amazon WorkSpaces Core usando:

- Studio
- Comandos do PowerShell

Nota:

Verifique as restrições do seu servidor proxy ou firewall e certifique-se de que os seguintes endereços possam ser contatados: `https://*.amazonaws.com` e `https://*.api.aws`. Além disso, certifique-se de que todos os endereços mencionados em Conectividade do serviço Citrix Gateway possam ser contatados.

Se estes não puderem ser contatados, isso poderá causar falha ao criar ou atualizar a conexão do host.

Criar uma conexão usando o Studio

1. navegar para a página **Hosting > Adicionar Conexão e Recursos**.
2. Na página **Conexão**, siga estas etapas para configurar a conexão:
    a. Selecione **Criar uma nova conexão**.

b. Em **Zona**, selecione o local do recurso que você configurou para seu ambiente AWS.

c. Selecione **Amazon WorkSpaces Core** como o tipo de conexão.

d. Selecione **Usar chave de acesso de usuário IAM** ou **Usar função IAM**.

   Para a chave de acesso de usuário IAM, forneça sua **chave de API** e **chave secreta** para o usuário IAM que possui a política de permissões IAM adequada para a Citrix gerenciar recursos em sua conta AWS.

   Para a função IAM, certifique-se de ter atribuído uma função IAM à instância do Citrix Cloud Connector com a política de permissões IAM adequada para a Citrix gerenciar recursos em sua conta AWS. Consulte Guia de autenticação baseada em função para obter mais informações.

e. Para rotear solicitações de API para a AWS por meio dos Citrix Cloud Connectors, selecione a caixa de seleção **Usar o proxy do sistema nos Citrix Cloud Connectors**. Isso garante que a conectividade AWS funcione corretamente quando os Cloud Connectors não tiverem acesso direto à Internet.

f. Insira um nome de conexão e clique em **Avançar**.

3. Na página **Local da Máquina Virtual**, especifique o local onde as VMs devem ser provisionadas. Selecione a região da nuvem, VPC e zona de disponibilidade (ou zona local) para criar novas VMs.
4. Na página **Rede**:

   a. Insira um nome para os recursos que você selecionou anteriormente na zona de disponibilidade (ou zona local).

   b. Selecione uma ou mais sub-redes na VPC que você configurou no menu anterior.

5. Clique nas páginas restantes até a página **Resumo**.
6. Clique em **Concluir** para criar a conexão de host com as instâncias gerenciadas do Amazon WorkSpaces Core.

CONSIDERAÇÕES IMPORTANTES

Ao criar uma conexão usando o Studio:

- Defina as permissões IAM adequadas para a Citrix gerenciar seus recursos AWS.
- Se você usa uma chave de acesso de usuário IAM para o Citrix gerenciar seus recursos AWS, você deve fornecer os valores da chave de API e da chave secreta. Você pode exportar o arquivo de chave contendo esses valores do AWS e depois importá-los. Você também deve

fornecer a região, zona de disponibilidade, nome da VPC, endereços de sub-rede, nome de domínio, nomes de grupos de segurança e credenciais.

- Se você usa uma função IAM para o Citrix gerenciar seus recursos AWS, você deve garantir que uma função com as permissões IAM adequadas seja atribuída a todos os seus Cloud Connector(s). Consulte o guia de autenticação baseada em função para obter mais informações.
- O arquivo de credenciais para a conta raiz do AWS (recuperado do console do AWS) não é formatado da mesma forma que os arquivos de credenciais baixados para usuários padrão do AWS. Portanto, o Citrix DaaS não pode usar o arquivo para preencher os campos de chave de API e chave secreta. Certifique-se de que você está usando arquivos de credenciais do AWS Identity Access Management (IAM).
- A zona pode ser uma zona de disponibilidade ou zona local.

Criar uma conexão usando PowerShell

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos do Citrix.
3. Execute os seguintes comandos. A seguir, um exemplo:

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$apiSecret = “bbbbb”

$secureKey = ConvertTo-SecureString -String $apiSecret

$zoneUid = "00000000-0000-0000-0000-000000000000"

$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath -ConnectionType
"AmazonWorkSpacesCoreMachineManagerFactory" -HypervisorAddress "
"https://workspaces-instances.$($cloudRegion).api.aws"" -Persist -Scope
@() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid



$hostingUnitName = "demo-hostingunit"

$availabilityzone = "us-east-1a"

$vpcName = "Default VPC"

$jobGroup = [Guid]::NewGuid()

$hostingUnitPath = "XDHyp:\HostingUnits\" + $HostingUnitName

$rootPath = $connectionPath + "\" + $vpcName + ".virtualprivatecloud\"

$availabilityZonePath = @($rootPath + $availabilityzone +
".availabilityzone")

$networkPaths = (Get-ChildItem $availabilityZonePath[0] | Where
ObjectType -eq "Network") | Select-Object -ExpandProperty FullPath #
will select all the networks in the availability zone



New-Item -Path $hostingUnitPath -AvailabilityZonePath
$availabilityZonePath -HypervisorConnectionName $connectionName
-JobGroup $jobGroup -PersonalvDiskStoragePath @() -RootPath $rootPath
-NetworkPath $networkPaths
```

Nota:

Para criar uma conexão usando a Autenticação Baseada em Função, especifique apiKey e apiSecret como `role_based_auth`.

Limitação

Se você alterar o nome de uma Virtual Private Cloud (VPC) do AWS no console do AWS, a unidade de hospedagem existente no Citrix Cloud™ será quebrada. Quando a unidade de hospedagem está quebrada, você não pode criar catálogos ou adicionar máquinas a catálogos existentes. Para resolver o problema, altere o nome da VPC do AWS de volta para o nome original.

Criar um ambiente seguro para tráfego gerenciado pelo AWS

Se você tiver um proxy configurado nos Cloud Connectors, então você deve criar a conexão de host para usar o proxy, de modo que as chamadas de API feitas pelo MCS sejam roteadas corretamente através do proxy. O MCS permite que o tráfego de rede (chamadas de API do Citrix Cloud para o hipervisor AWS) seja roteado através dos Cloud Connectors em seu ambiente.

A conexão de host pode ler o valor do proxy do sistema WinHTTP que é configurado durante a instalação do Cloud Connector. Você pode configurar o proxy usando o Studio ou definindo a propriedade personalizada `UseSystemProxyForHypervisorTrafficOnConnectors` como `True` ao criar ou atualizar uma conexão de host usando PowerShell.

> **Nota:**
>
> Se seu ambiente usa um proxy, certifique-se de que a inspeção SSL esteja desabilitada ou que a conexão SSL permaneça inalterada para `<https://workspaces-instances.*.api.aws/>`.

CRIAR UMA CONEXÃO DE HOST CONFIGURADA COM O PROXY

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute os comandos PowerShell para configurar o proxy. Por exemplo:

```
$connectionName = "demo-hostingconnection"

$cloudRegion = "us-east-1"

$apiKey = "aaaaaaaaaaaaaaaaaaaa"

$zoneUid = "00000000-0000-0000-0000-000000000000"
```

```
$securePassword = Read-Host 'Please enter your secret key'
-AsSecureString

$connectionPath = "XDHyp:\Connections\" + $connectionName



$customProperties = @"

<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />

</CustomProperties>

"@
```

4. Crie uma conexão de hospedagem. Por exemplo:

```
$connection = New-Item -Path $connectionPath `

-ConnectionType "Custom" -PluginId
"AmazonWorkSpacesCoreMachineManagerFactory" `

-HypervisorAddress "https://workspaces-instances.$
($cloudRegion).api.aws" `

-CustomProperties> $customProperties `

-Persist -Scope @()`

-UserName $apiKey -SecurePassword $securePassword `

-ZoneUid $zoneUid
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

Para habilitar o proxy para uma conexão de host existente, consulte Habilitar o proxy em uma conexão existente.

Provisionamento entre contas

Existem casos de uso em que os Cloud Connectors gostariam de ser colocados em uma conta AWS separada (conta de serviços compartilhados ou conta de componentes de site) com funções IAM que têm acesso entre contas (função IAM entre contas) e catálogos de máquinas provisionados por MCS em uma conta AWS secundária separada (contas de cargas de trabalho), sem a necessidade de Cloud Connectors adicionais nas contas separadas. Para suportar tais cenários, este recurso usa o emparelhamento de VPC e acesso entre contas usando funções IAM para tornar o provisionamento entre diferentes contas AWS possível para empresas que gerenciam múltiplas contas AWS.

Com emparelhamento de VPC, você pode ter seu Cloud Connector e VMs provisionadas em diferentes regiões ou contas capazes de se comunicar entre si.

Com acesso entre contas usando funções IAM, você permite que a conta primária (conta do Cloud Connector) assuma uma função IAM para acessar recursos AWS na conta secundária (VMs do catálogo de máquinas).

Para permitir que o Cloud Connector acesse os recursos da conta secundária, crie uma conexão de host após assumir a função IAM da conta secundária.

Pré-requisitos

Configure o seguinte antes de criar uma conexão de host para provisionamento entre contas:

- Configure o emparelhamento de VPC e os grupos de segurança em ambas as regiões ou contas. Consulte Configurar emparelhamento de VPC.
- Delegue o acesso entre contas usando funções do IAM. Consulte Delegar acesso entre contas usando função do IAM.

Configurar emparelhamento de VPC

Vamos supor que a VPC A esteja na conta principal (Conta A) e tenha os Cloud Connectors e o Active Directory. A VPC B está na conta secundária (Conta B), onde você deseja provisionar as VMs.

Para configurar uma conexão de emparelhamento de VPC entre a Conta A e a Conta B, faça o seguinte:

1. Crie uma conexão de emparelhamento de VPC. Consulte:
   - Conta diferente, mesma região
   - Conta diferente, região diferente
2. Vá para sua VPC A e para a tabela de rotas associada à sub-rede pública.
3. Clique em **Editar Rotas > Adicionar rota**. Adicione o bloco CIDR da VPC B na coluna **Destino** e adicione o emparelhamento de VPC que você criou na coluna **Alvo**.
4. Repita as Etapas 2 e 3, mas com as sub-redes privadas para VPC A e VPC B (adicione o bloco CIDR da VPC A). Consulte Atualizar suas tabelas de rotas para uma conexão de emparelhamento de VPC.
5. Vá para o grupo de segurança privado associado à VPC A.
6. Selecione **Ações** e, em seguida, **Editar regras de entrada**.
7. Selecione **Adicionar regra**. Para o tipo, selecione **Todo o tráfego** e, em seguida, na **Coluna de Origem** adicione:
   - Se for uma região diferente, adicione o Bloco CIDR da VPC B.
   - Se for uma conta diferente, mas na mesma região, adicione o ID da conta e o ID do grupo de segurança privado da VPC B separados por uma barra (Exemplo, 123456789012/sg-1a2b3c4d)
8. Repita os Passos 5 a 7, mas com o grupo de segurança privado para a VPC B (mas adicione o Bloco CIDR da VPC A ou o ID da conta da VPC A e o ID do grupo de segurança privado da mesma região, mas de uma conta diferente). Consulte Atualize seus grupos de segurança para referenciar grupos de segurança pares.

Nota:

Não há cobrança para criar uma conexão de emparelhamento de VPC. No entanto, embora o emparelhamento de VPC dentro de uma zona de disponibilidade seja gratuito, aplicam-se cobranças quando a transferência de dados por uma conexão de emparelhamento de VPC ocorre em várias zonas de disponibilidade e regiões. Consulte Preços para uma conexão de emparelhamento de VPC.

Delegar acesso entre contas usando funções IAM

Após configurar o emparelhamento de VPC entre contas, você delega o acesso entre contas usando funções IAM.

Com o acesso entre contas usando funções IAM, você permite que a conta primária (conta do Cloud Connector) assuma uma função IAM para acessar recursos AWS na conta secundária (VMs do catálogo de máquinas).

Para acessar recursos entre contas, faça o seguinte:

> **Lembre-se:**

> Assumindo que a VPC A está na conta primária (Conta A) e possui o Cloud Connector e o Active Directory. A VPC B está na conta secundária (Conta B) onde você deseja provisionar as VMs

1. Configure o emparelhamento de VPC entre contas com as etapas mencionadas anteriormente.
2. Crie uma função e política IAM na Conta B com permissões IAM mínimas da Citrix. Consulte Tutorial IAM: Delegar acesso entre contas AWS usando funções IAM. Digamos que o ARN desta função seja "arn:aws:iam::5678:role/citrix-role".
3. Adicione a política de confiança à função "arn:aws:iam::5678:role/citrix-role" para que ela possa ser acessada pela função da Conta A "arn:aws:iam::1234:role/primary-account-citrix-role" conforme - Acesso a recursos entre contas no IAM.
4. Crie a função e política IAM na Conta A com o nome mencionado anteriormente "primary-account-citrix role", que pode assumir a função IAM e passar a função IAM da Conta B (arn:aws:iam::5678:role/citrix-role).
5. Atribua a função "arn:aws:iam::1234:role/primary-account-citrix-role" a todos os Cloud Connectors na Conta A.

Os Cloud Connectors agora podem assumir a função da Conta B ("arn:aws:iam::5678:role/citrix-role").

Criar conexão de host para provisionamento entre contas

Crie uma conexão de host na conta secundária (Conta B) onde você deseja provisionar as VMs. Isso permite que os Cloud Connectors da Conta A acessem os recursos na Conta B após assumir a função da Conta B.

Use comandos PowerShell para criar a conexão de host e adicionar as duas propriedades personalizadas a seguir:

- `CrossAccountRoleArn`: Se você não fornecer a propriedade `CrossAccountRoleArn`, a conexão de host regular será criada. Neste caso, `MaximumAssumeRoleDurationInSeconds` é ignorado mesmo que seja fornecido.
- `MaximumAssumeRoleDurationInSeconds`: `DurationInSeconds` deve estar entre 900 segundos e 3600 segundos. O padrão é 900 segundos. Se você fornecer um valor maior que 3600, então `DurationInSeconds` será definido como 3600.

Exemplo:

```
$connectionName = "cross-account-conn"

$cloudRegion = "us-east-1"

$apiKey = "role_based_auth"

$secretKey = "role_based_auth"

$zoneUid = "xxxxxx"

$secureKey = (ConvertTo-SecureString -String $secretKey -AsPlainText
-Force)

$connectionPath = "XDHyp:\Connections\" + $connectionName

$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CrossAccountRoleArn"
Value="arn:aws:iam::5678:role/citrix-role" /><Property
xsi:type="StringProperty" Name="MaximumAssumeRoleDurationInSeconds"
Value="3600" />

"</CustomProperties>'



$connection = New-Item -Path $connectionPath -ConnectionType
"AmazonWorkSpacesCoreMachineManagerFactory" -HypervisorAddress "https://
```

```
workspaces-instances.$($cloudRegion).api.aws" -Persist -Scope @()
-UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
-CustomProperties $customProperties



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

Após a criação da conexão de host, crie unidades de hospedagem usando o Studio ou PowerShell. No entanto, selecione VPC e Redes.

Ignorar Cloud Connectors para solicitações de API da AWS

Em ambientes de Instância Gerenciada (MI) do Amazon WorkSpaces Core, o plug-in do Citrix Machine Creation Services (MCS) normalmente reside no Delivery Controller e roteia as solicitações de API da AWS através do Citrix Cloud Connector via proxy.

Você pode configurar conexões de host para ignorar o Cloud Connector para solicitações de API da AWS. Quando esse recurso é ativado, o plug-in faz chamadas de API — incluindo aquelas para provisionamento e gerenciamento de energia — diretamente do DDC para os serviços da AWS (como Amazon EC2, EBS e instâncias do WorkSpaces), removendo a dependência de passar pelo Cloud Connector via proxy.

Benefícios

- Reduzir a dependência de chamadas de API da AWS em Cloud Connectors: Remover a dependência da API da AWS no Cloud Connector é um passo fundamental para clientes que visam reduzir sua pegada de infraestrutura local ou na nuvem.
- Consumo de Recursos Reduzido: Menos tráfego através do Cloud Connector reduz os requisitos de computação para a VM do Connector, potencialmente levando a economias de custo.
- Flexibilidade Operacional: Oferece maior disponibilidade ao remover um ponto potencial de falha (o caminho do proxy Cloud Connector/NGS) para tarefas críticas de gerenciamento de energia e provisionamento.

Limitações e considerações

Antes de habilitar este recurso, considere os seguintes requisitos e limitações:

- Autenticação: A autenticação baseada em função (funções IAM) não é suportada ao ignorar o Cloud Connector. Você deve configurar a instalação apenas para chaves de acesso de usuário IAM.
- Escopo do ambiente: Este recurso é exclusivo para instâncias gerenciadas do Amazon WorkSpaces Core (MI). Não é suportado para conexões de host AWS EC2 padrão.
- Requisitos de rede: O DDC deve ter um caminho de rede direto para os endpoints do serviço AWS.
- Saúde do local do recurso: Se um Cloud Connector foi originalmente provisionado no local do recurso, ele deve permanecer ligado. Componentes não-MCS e verificações de saúde ainda dependem do Cloud Connector, se ele existir.
- Recursos não suportados:
  - Provisionamento entre contas
  - Uso de proxy do sistema
- Requisitos do conector: Embora este recurso remova a dependência da API, existem outras configurações necessárias para reduzir as dependências dos Cloud Connectors (os requisitos para Cloud Connectors podem não se limitar aos listados aqui):
  - Ingresso no domínio: Usando máquinas não ingressadas no domínio ou ingressadas no Microsoft Entra híbrido.
  - Registro de VDA: Habilitando o Rendezvous V2 (comunicação direta do DDC para o VDA via WebSockets) para registro de VDA.

Criar uma conexão de host com bypass de API

Ao criar uma conexão de host na Configuração Completa (Studio), agora você pode selecionar locais de recurso do Amazon WorkSpaces Core mesmo que nenhum Cloud Connector esteja presente nesse local.

Para habilitar o bypass via PowerShell, use a propriedade personalizada `BypassConnectorForAwsApiRequests`.

Exemplo de PowerShell:

```
$custProp = '<CustomProperties xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation">

  <Property xsi:type="StringProperty"
```

```
Name="BypassConnectorForAwsApiRequests" Value="true" />

</CustomProperties>'



$connectionName = "MyWSCConnection"

$cloudRegion = "us-east-1"

$apiKey = "YOUR_IAM_ACCESS_KEY"

$zoneUid = (Get-ConfigZone | Where-Object {$_.Name -eq
"MyResourceLocation"}).Uid

$securePassword = Read-Host 'Enter your IAM Secret Key' -AsSecureString



$connectionPath = "XDHyp:\Connections\" + $connectionName



$connection = New-Item -Path $connectionPath `

    -ConnectionType "Custom" `

    -PluginId "AmazonWorkSpacesCoreMachineManagerFactory" `

    -HypervisorAddress "https://workspaces-instances.$
($cloudRegion).api.aws" `

    -Persist -Scope @() `

    -CustomProperties $custProp `

    -UserName $apiKey -SecurePassword $securePassword `

    -ZoneUid $zoneUid
```

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

Gerenciar conexões existentes

Você pode habilitar ou desabilitar o recurso de bypass para conexões de host existentes.

- Habilitando em conexões existentes: Você pode modificar as propriedades personalizadas de uma conexão existente para incluir `BypassConnectorForAwsApiRequests = true.`.
- Desabilitando: Se desabilitado, o DDC retoma o roteamento de chamadas de API da AWS através do Cloud Connector via proxy NGS. Observe que isso requer que um Cloud Connector funcional e um caminho de proxy NGS estejam disponíveis no local do recurso.

Solução de problemas

Se você tentar habilitar a propriedade de bypass em condições não suportadas, o sistema retornará um erro de validação:

- Funções IAM/Contas Cruzadas/Proxy: Se habilitado juntamente com funções IAM, provisionamento entre contas ou proxies de sistema, o `New-Item` comando falha com:

  ```
  AmazonWorkSpacesCoreException: Bypassing the Cloud Connector For AWS
  API requests is not supported for IAM roles, Cross-Account provisioning
  and System Proxy.
  ```

- Tipo de Conexão Não Suportado: Se aplicado a uma conexão padrão do Amazon EC2 (AWS), o sistema falha com:

  ```
  AmazonWorkSpacesCoreException: Bypassing the Cloud Connector For AWS
  API requests is not supported for EC2 host connection.
  ```

Editar uma conexão

Você pode editar uma conexão de host existente para:

- Modificar a opção de fornecer permissões IAM para a Citrix gerenciar recursos
- Modificar o número máximo de ações simultâneas (ou máquinas concorrentes) por conexão de hospedagem
- Modificar o escopo.

- Configurar o número máximo de grupos de segurança permitidos por interface de rede elástica (ENI) usando o comando PowerShell
- Habilitar o proxy para criar um ambiente seguro para o tráfego gerenciado pela AWS

Editar opções para fornecer permissões IAM

1. Clique com o botão direito do mouse em uma conexão Amazon WorkSpaces Core existente.
2. Na página **Propriedades da Conexão**, clique em **Editar configurações**.
3. Selecione uma das opções para fornecer permissões IAM para a Citrix gerenciar recursos. Insira os detalhes necessários e clique em **Salvar**.

Modificar o número máximo de ações simultâneas

Ao criar conexões de host no Studio para instâncias gerenciadas do Amazon WorkSpaces Core, os seguintes valores padrão são exibidos:

OPÇÃO	ABSOLUTO	PORCENTAGEM
Ações simultâneas (todos os tipos)	125	100
Máximo de novas ações por minuto	150	n/d
Máximo de operações de provisionamento simultâneas	150	n/d

O MCS suporta 150 operações de provisionamento simultâneas máximas por padrão.

Você pode configurar esses valores acessando a seção **Avançado** do Citrix Studio na tela **Editar Conexão**:

Alternativamente, você pode usar o SDK do PowerShell Remoto para definir o número máximo de operações simultâneas para configurações ideais por ambiente.

Use a propriedade personalizada do PowerShell, `MaximumConcurrentProvisioningOperations`, para especificar o número máximo de operações de provisionamento AWS simultâneas.

Antes da configuração:

- Certifique-se de ter instalado o SDK do PowerShell para a Nuvem.

- Entenda que o valor padrão para `MaximumConcurrentProvisioningOperations` é 150.

Execute as seguintes etapas para personalizar o valor `MaximumConcurrentProvisioningOperations`:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Insira `cd xdhyp:\Connections\`.
4. Digite `dir` para listar as conexões.
5. Alterar ou inicializar a string de Propriedades Personalizadas:
   - Se a string de Propriedades Personalizadas tiver um valor, copie as Propriedades Personalizadas para o Bloco de Notas. Em seguida, altere a propriedade `MaximumConcurrentProvisioningOperations` para o seu valor preferido. Você pode inserir um valor no intervalo de 1 a 1000. Por exemplo, `<Property xsi:type="IntProperty" Name="MaximumConcurrentProvisioningOperations" Value="xyz"/>`.
   - Se a string de Propriedades Personalizadas estiver vazia ou nula, você deve inicializar a string inserindo a sintaxe apropriada para o esquema e para a propriedade `MaximumConcurrentProvisioningOperations`.
6. Na janela do **PowerShell**, cole as Propriedades Personalizadas modificadas do Bloco de Notas e atribua uma variável às Propriedades Personalizadas modificadas. Se você inicializou as Propriedades Personalizadas, adicione as seguintes linhas após a sintaxe:

   ```
   $customProperties = '<CustomProperties xmlns="http://
   schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
   www.w3.org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'
   ```

   Esta string define a propriedade `MaximumConcurrentProvisioningOperations` como 100. Na string de Propriedades Personalizadas, você deve definir a propriedade `MaximumConcurrentProvisioningOperations` para um valor que se alinhe às suas necessidades.
7. Digite `Get-XDAuthentication`, que solicitará suas credenciais.

8. Execute `$cred = Get-Credential`, que pode solicitar apenas uma Senha (ou um Nome e Senha). Você também pode ser solicitado a fornecer o ID do aplicativo e o segredo associado. Para conexões que usam autenticação baseada em função, **role_based_auth** é o Nome e a Senha. Caso contrário, insira o ID da API AWS e o segredo.
9. Execute `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`. Você deve definir o <*connection-name*> para o nome da conexão.
10. Digite `dir` para verificar a string CustomProperties atualizada.

Configurar grupos de segurança por interface de rede

Ao editar uma conexão de host, agora você pode configurar o número máximo de grupos de segurança permitidos por interface de rede elástica (ENI) usando um comando PowerShell. Para obter informações sobre os valores de cota de grupos de segurança da AWS, consulte Grupos de segurança.

Para configurar grupos de segurança por interface de rede:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute `cd xdhyp:\Connections\`.
4. Execute `dir` para listar as conexões.
5. Execute o seguinte comando PowerShell para configurar grupos de segurança por interface de rede:

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws -Name
"Citrix_MachineManagement_Options" -Value "
AwsMaxENISecurityGroupLimit=<number>"
```

> **Nota:**
>
> Se você não definir um valor para `AwsMaxENISecurityGroupLimit`, ele assumirá o valor padrão de 5.

Habilitar o proxy em uma conexão existente

1. Abra uma janela do PowerShell.

2. Execute os seguintes comandos.

```
Add-PSSnapin citrix*.

cd XDHyp:\Connections\

dir
```

3. Copie o `CustomProperties` da conexão para um bloco de notas e anexe a configuração de propriedade `<Property xsi:type="StringProperty" Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />` ao `CustomProperties` para habilitar o proxy.
4. Na janela do PowerShell, atribua uma variável às propriedades personalizadas modificadas. Por exemplo:

```
$customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation">

<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />

</CustomProperties>'
```

5. Insira `Get-XDAuthentication`, que solicitará suas credenciais.
6. Execute `$cred = Get-Credential`, que pode solicitar apenas uma Senha (ou um Nome e Senha). Você também pode ser solicitado a informar o ID do aplicativo e o segredo associado. Para conexões que usam autenticação baseada em função, `role_based_auth` é tanto o Nome quanto a Senha. Caso contrário, insira o ID e o segredo da API da AWS.
7. Execute `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`. Você deve definir o `<connection-name>` para o nome da conexão.
8. Insira `dir` para verificar a string `CustomProperties` atualizada.

URL do endpoint de serviço

URL de endpoint de serviço de zona padrão

Quando você usa o MCS, uma nova conexão de instâncias gerenciadas do Amazon WorkSpaces Core é adicionada com uma chave de API e um segredo de API. Com essas informações, juntamente com a conta autenticada, o MCS consulta a AWS para as regiões e zonas suportadas usando chamadas de API do AWS EC2 e do Amazon WorkSpaces Core Managed Instances. A consulta é feita usando uma URL de endpoint de serviço de instâncias do Workspace `<https://workspaces-instances.us-east-1.api.aws/>` e um endpoint de serviço EC2 https:/ec2.us-east-1.api.aws/.

> **Nota:**
>
> Certifique-se de que `<https://workspaces-instances.us-east-1.api.aws/>` esteja acessível.

URL de endpoint de serviço não padrão

Pode haver situações em que você não precise da URL de endpoint de serviço da AWS escolhida automaticamente para a conexão. Nesses casos, você pode usar o Citrix Cloud SDK e o PowerShell para criar uma conexão com uma URL de endpoint de serviço não padrão. Por exemplo, para criar uma conexão usando a URL de endpoint de serviço `https://ec2.cn-north-1.amazonaws.com.cn`:

1. Configure o Cloud Connector hospedado na AWS e certifique-se de que ele tenha conectividade.
2. Execute os seguintes comandos do PowerShell para ver a lista de Cloud Connectors.

```
PS C:\> asnp citrix.*

PS C:\> Get-XDAuthentication

PS C:\> Get-ConfigEdgeServer
```

3. Encontre o ZoneUid do Cloud Connector recém-criado e insira-o nos seguintes comandos do PowerShell. Substitua os itens em itálico pelos respectivos valores.

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUid ZoneUid -Name
“My New Connection” -ConnectionType "Custom" -HypervisorAddress
@("https://workspaces-instances.$($cloudRegion).api.aws")-PluginId
"AmazonWorkSpacesCoreMachineManagerFactory" -UserName “APIkey”
-Password “API Secret” -Persist



PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hyp. HypervisorConnectionUid
```

4. Atualize a guia **Hospedagem** para verificar se a conexão foi criada.
5. Adicione um local de recurso usando a nova conexão.

Permissões AWS necessárias

Esta seção contém a lista completa de permissões da AWS. Use o conjunto completo de permissões conforme fornecido na seção para que a funcionalidade funcione corretamente.

> **Nota:**
>
> A permissão `iam:PassRole` é necessária apenas para usar funções IAM para que a Citrix gerencie recursos.

Criando uma conexão de host

Uma nova conexão de host é adicionada usando as informações obtidas da AWS.

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "workspaces-instances:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Gerenciamento de energia de VMs

As VMs são ligadas ou desligadas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeInstances",,
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "ec2:DescribeInstanceStatus"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
           "Action": [
               "workspaces-instances:*"
           ],
           "Effect": "Allow",
            "Resource": "*"
       }


    ]


}
```

Criando, atualizando ou excluindo VMs

Um catálogo de máquinas é criado, atualizado ou excluído com VMs provisionadas como instâncias AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
```

```
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
```

```
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
```

```
                "workspaces-instances:*"

            ],

            "Effect": "Allow",

            "Resource": "*"

        },

        {

            "Effect": "Allow",

            "Action": [

                "iam:GetAccountSummary",

                "ec2:CopyImage"

            ],

            "Resource": "*"

        },



    ]

}
```

Nota:

- A seção EC2 relacionada a SecurityGroups só é necessária se um Grupo de Segurança de Isolamento precisar ser criado para a VM de Preparação durante a criação do catálogo. Uma vez feito isso, essas permissões não são mais necessárias.

- As permissões EC2 `CopyImage` e IAM `GetAccountSummary` são necessárias apenas ao compartilhar imagens preparadas entre regiões. Consulte Compartilhar imagens preparadas entre zonas de disponibilidade e regiões.

Upload e download direto de disco

As seguintes permissões devem ser adicionadas à política:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

Criptografia EBS de volumes criados

O EBS pode criptografar automaticamente volumes recém-criados se a AMI estiver criptografada, ou se o EBS estiver configurado para criptografar todos os novos volumes. No entanto, para implementar a funcionalidade, as seguintes permissões devem ser incluídas na política IAM.

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",
```

```
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
    ]
}
```

Nota:

As permissões podem ser limitadas a chaves específicas, incluindo um bloco de Recurso e Condição a critério do usuário. Por exemplo, **Permissões KMS com Condição**:

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
```

```
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

A seguinte declaração de política de chave é a política de chave padrão completa para chaves KMS que é necessária para permitir que a conta use políticas IAM para delegar permissão para todas as ações (kms:*) na chave KMS.

```
{

"Sid": "Enable IAM policies",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::111122223333:root"

},

"Action": "kms:",

"Resource": ""

}
```

Para obter mais informações, consulte a documentação oficial do AWS Key Management Service.

Autenticação baseada em função IAM

As seguintes permissões são adicionadas para suportar a autenticação baseada em função.

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]
```

```
}
```

Política de permissões IAM mínima

O JSON a seguir pode ser usado para todos os recursos atualmente suportados. Você pode criar conexões de host, criar, atualizar ou excluir VMs e fazer gerenciamento de energia usando esta política. A política pode ser aplicada aos usuários conforme explicado nas seções Definir permissões IAM ou você também pode usar a autenticação baseada em função selecionando **Usar função IAM** ao configurar uma conexão de host.

Importante:

Para usar **funções IAM para o Citrix gerenciar recursos**, primeiro configure a função IAM desejada na instância EC2 do conector de nuvem ao configurar o conector de nuvem. Usando o Citrix Studio, adicione a conexão de hospedagem e selecione a opção **Usar função IAM**. Uma conexão de hospedagem com essas configurações usa então a autenticação baseada em função.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
```

```
                "ec2:CreateLaunchTemplate",

                "ec2:CreateNetworkInterface",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteLaunchTemplate",

                "ec2:DeleteNetworkInterface",

                "ec2:DeleteSecurityGroup",

                "ec2:DeleteSnapshot",

                "ec2:DeleteTags",

                "ec2:DeleteVolume",

                "ec2:DeregisterImage",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",
```

```
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
```

```
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-instances:*"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetAccountSummary",
                "ec2:CopyImage"
            ],
            "Resource": "*"
        }

    ]
}
```

Nota:

- A seção EC2 relacionada a SecurityGroups é necessária apenas se um Grupo de Segurança de Isolamento precisar ser criado para a VM de Preparação durante a criação do catálogo. Uma vez feito isso, essas permissões não são mais necessárias.
- A seção KMS é necessária apenas ao usar a criptografia de volume EBS.
- A seção de permissão `iam:PassRole` é necessária apenas para usar funções IAM para o Citrix gerenciar recursos.
- Permissões específicas em nível de recurso podem ser adicionadas em vez de acesso total, com base em seus requisitos e ambiente. Consulte os documentos da AWS Desmistificando as Permissões em Nível de Recurso do EC2 e Gerenciamento de acesso para recursos da AWS para obter mais detalhes.

- Use as permissões `ec2:CreateNetworkInterface` e `ec2:DeleteNetworkInterface` apenas se estiver usando o método de worker de volume.

Onde ir em seguida

- Para criar imagens preparadas, consulte Criar uma imagem preparada para instâncias gerenciadas do Amazon WorkSpaces Core

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização AWS
- Para exemplos de PowerShell do GitHub do Amazon WorkSpaces Core, consulte citrix-mcs-sdk-samples-Amazon WorkSpaces Core.

Conexão com ambientes de nuvem do Google

(/pt-br/citrix-daas/install-configure/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de nuvem do Google.

Nota:

Antes de criar uma conexão com ambientes de nuvem do Google, você precisa primeiro concluir a configuração da sua conta do Google Cloud como um local de recurso. Consulte (/pt-br/citrix-daas/install-configure/resource-location/google.html).

Adicionar uma conexão

No Studio, siga as orientações em (/pt-br/citrix-daas/install-configure/connections.html). A descrição a seguir o orienta na configuração de uma conexão de hospedagem:

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione **Adicionar Conexão e Recursos** na barra de ações.
3. Na página **Conexão**, selecione **Criar uma nova Conexão** e **ferramentas de provisionamento Citrix™**, e então selecione **Avançar**.

- **Nome da zona**. Selecione uma zona (equivalente a um local de recurso) onde você deseja que seus recursos de host residam. As zonas são criadas automaticamente quando você cria um local de recurso e adiciona um Cloud Connector a ele. Para obter mais informações, consulte (/pt-br/citrix-daas/manage-deployment/zones.html).
- **Tipo de conexão**. Selecione **Google Cloud Platform** no menu.
- **Chave da conta de serviço**. Importe a chave contida no seu arquivo de credenciais do Google (.json). Você pode colar a chave do arquivo de credenciais ou navegar até o arquivo de credenciais. Para colar a chave:

  a. Localize seu arquivo de credenciais

  b. Abra o arquivo com o Bloco de Notas (ou qualquer editor de texto)

  c. Copie o conteúdo.

  d. Volte para a página **Conexão**, selecione **Adicionar chave**, cole o conteúdo e, em seguida, selecione **Concluído**.

- **ID da conta de serviço**. O campo é preenchido automaticamente com as informações da chave da conta de serviço.
- **Nome da conexão**. Digite um nome para a conexão.
- **Encaminhar tráfego por meio de Citrix Cloud Connectors**. Para encaminhar as solicitações de API por meio de um Citrix Cloud Connector™ disponível, marque esta caixa de seleção. Quando os Cloud Connectors não têm acesso direto à internet, você pode selecionar **Usar o proxy configurado nos Citrix Cloud Connectors** para garantir que a conectividade GCP funcione corretamente por meio dos Citrix Cloud Connectors. Você também pode marcar a caixa de seleção **Habilitar o Google Cloud Build para usar pools privados** para uma camada adicional de segurança.

  Alternativamente, você pode habilitar esse recurso usando o PowerShell. Para obter mais informações, consulte Criar um ambiente seguro para tráfego gerenciado por GCP.

> **Nota:**
>
> Esta opção está disponível somente quando há Citrix Cloud™ Connectors ativos em sua implantação. Atualmente, esse recurso não é compatível com Connector Appliances.

- **Criar máquinas virtuais usando**. Selecione um método para criar máquinas virtuais.

4. Na página **Região**, selecione um nome de projeto no menu, selecione uma região que contenha os recursos que você deseja usar e, em seguida, selecione **Avançar**.
5. Na página **Rede**, digite um nome para os recursos, selecione uma rede virtual no menu, selecione um subconjunto e, em seguida, selecione **Avançar**. O nome do recurso ajuda a identificar a combinação de região e rede. Redes virtuais com o sufixo *(Compartilhado)* anexado ao seu nome representam VPCs compartilhadas. Se você configurar uma função IAM no nível da sub-rede para uma VPC compartilhada, apenas sub-redes específicas da VPC compartilhada aparecerão na lista de sub-redes.

   Nota:

   - O nome do recurso pode conter 1 a 64 caracteres e não pode conter apenas espaços em branco ou os caracteres `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`.

6. Na página **Resumo**, confirme as informações e, em seguida, selecione **Concluir** para sair da janela **Adicionar Conexão e Recursos**.

Depois de criar a conexão e os recursos, a conexão e os recursos criados são listados. Para configurar a conexão, selecione a conexão e, em seguida, selecione a opção aplicável na barra de ações.

Da mesma forma, você pode excluir, renomear ou testar os recursos criados sob a conexão. Para fazer isso, selecione o recurso sob a conexão e, em seguida, selecione a opção aplicável na barra de ações.

Criar um ambiente seguro para o tráfego gerenciado do GCP

Você pode permitir apenas o acesso privado do Google aos seus projetos do Google Cloud. Essa implementação aprimora a segurança para manipular dados confidenciais. Para fazer isso:

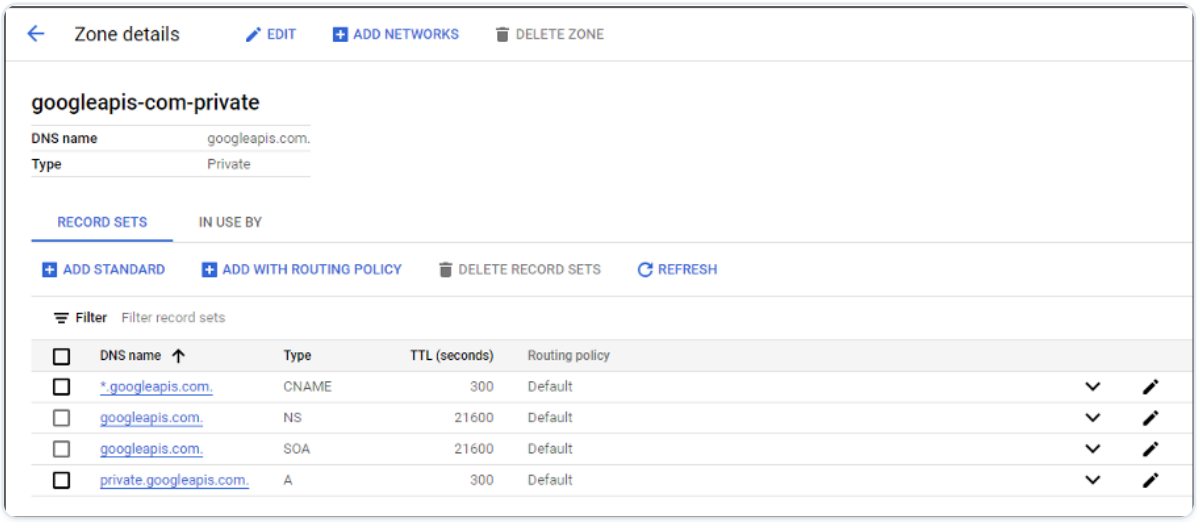
1. Instale os Cloud Connectors na VPC onde você deseja aplicar os controles de serviço da VPC. Consulte Controles de Serviço da VPC para obter mais informações.
2. Adicione `ProxyHypervisorTrafficThroughConnector` em `CustomProperties` no caso de implantação do Citrix Cloud. Se você estiver usando um pool de trabalhadores privado, adicione `UsePrivateWorkerPool` em `CustomProperties`. Para obter informações sobre o pool de trabalhadores privado, consulte Visão geral de pools privados.

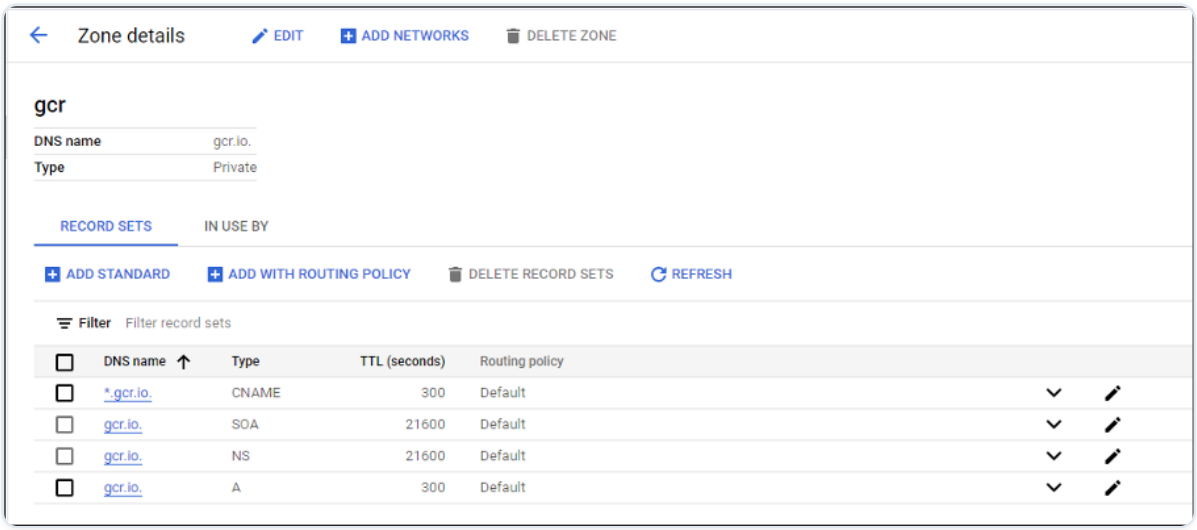
> **Nota:**
>
> Atualmente, este recurso não é compatível com o Connector Appliance.

Requisitos para criar um ambiente seguro para o tráfego gerenciado do GCP

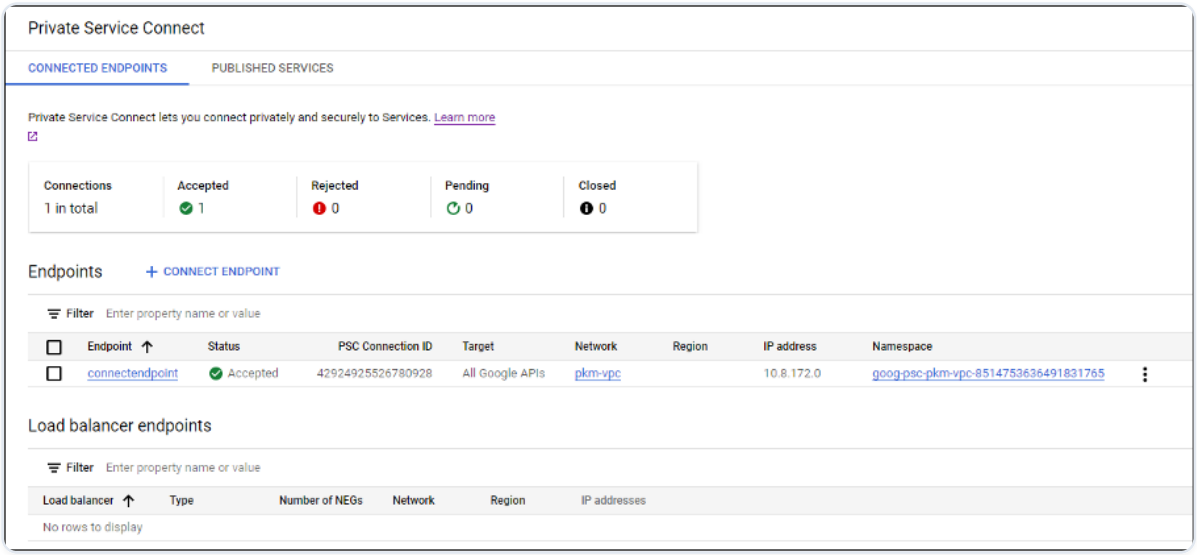
Os requisitos para criar um ambiente seguro para o tráfego gerenciado do GCP são:

- Certifique-se de que a conexão de hospedagem esteja no modo de manutenção ao atualizar as propriedades personalizadas.
- Para usar pools de trabalhadores privados, as seguintes alterações são necessárias:
  - Para a conta de serviço do Citrix Cloud, adicione as seguintes funções IAM:
    - Conta de Serviço do Cloud Build
    - Administrador de Instância de Computação
    - Usuário da Conta de Serviço
    - Criador de Token da Conta de Serviço
    - Proprietário do WorkerPool do Cloud Build
  - Crie a Conta de Serviço do Citrix Cloud no mesmo projeto que você usa para criar uma conexão de hospedagem.
  - Configure zonas DNS para `private.googleapis.com` e `gcr.io` conforme descrito em Configuração de DNS.

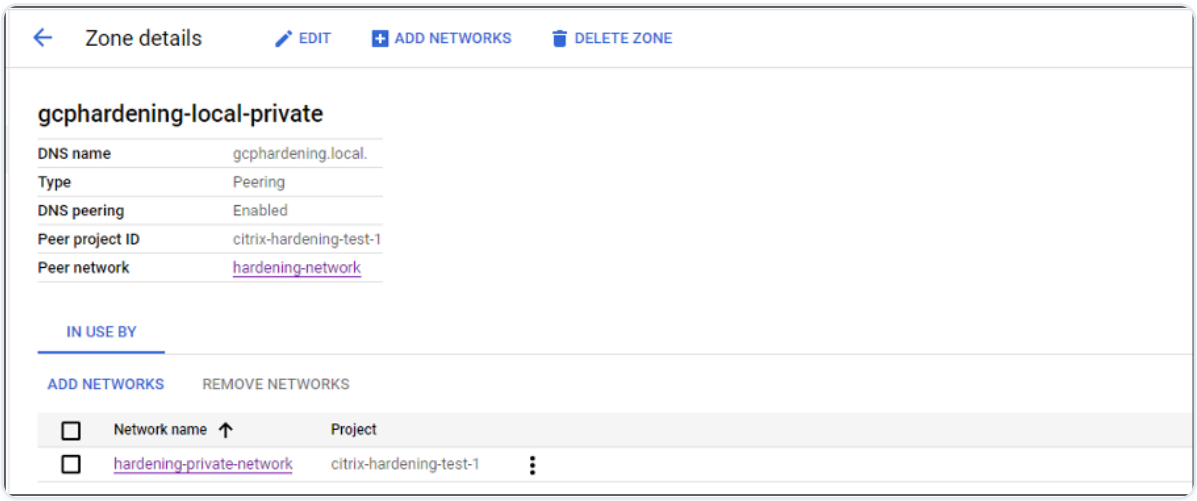




- Configure a Tradução de Endereços de Rede (NAT) privada ou use a conexão de serviço privada. Para obter mais informações, consulte Acessar APIs do Google por meio de endpoints.



- Se estiver usando uma VPC emparelhada, crie um emparelhamento de zona do Cloud DNS para a VPC emparelhada. Para obter mais informações, consulte Criar uma zona de emparelhamento.



- Nos controles de serviço da VPC, configure regras de Egress para que as APIs e VMs possam se comunicar com a internet. As regras de Ingress são opcionais. Por exemplo:

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:

Projects =

All projects

Service =

Service name: All services
```

Habilitar o proxy

Para habilitar o proxy, defina as propriedades personalizadas da seguinte forma na conexão do host:

1. Abra uma janela do PowerShell no host do Delivery Controller ou use o SDK do PowerShell Remoto. Para obter mais informações sobre o SDK do PowerShell Remoto, consulte SDKs e APIs.
2. Execute os seguintes comandos:
   a. `Add-PSSnapin citrix*`

b. `cd XDHyp:\Connections\`

c. `dir`

3. Copie o `CustomProperties` da conexão para um bloco de notas.
4. Anexe a configuração da propriedade da seguinte forma:

   - No caso de implantação em nuvem (usando pools públicos): Anexe a configuração da propriedade `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>` ao `CustomProperties` para habilitar o proxy. Por exemplo:

     ```
     <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance" xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

     <Property xsi:type="StringProperty"
     Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>

     </CustomProperties>
     ```

     Permita a regra de entrada para a Conta de Serviço do Cloud Build no perímetro de serviço da VPC. Por exemplo:

     ```
     Ingress Rule 1

     From:

     Identities:

     <ProjectID>@cloudbuild.gserviceaccount.com

     Source > All sources allowed

     To:

     Projects =

     All projects

     Services =
     ```

```
Service name: All services
```

Para obter informações sobre o perímetro de serviço da VPC, consulte Detalhes e configuração do perímetro de serviço.

- No caso de um pool de trabalhadores privado em uma implantação em nuvem, anexe a configuração da propriedade `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>` e `<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>` ao `CustomProperties` para habilitar o proxy. Por exemplo:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>

<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
Value="True"/>

</CustomProperties>
```

5. Na janela do PowerShell, atribua uma variável às propriedades personalizadas modificadas. Por exemplo: `$customProperty = '<CustomProperties…</CustomProperties>'`.
6. Execute `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`.
7. Execute `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`.
8. Execute `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`.
9. Execute o seguinte para atualizar uma conexão de host existente:

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION
NAME HERE>') -SecurePassword $securePassword -UserName
$gcpServiceAccount -CustomProperties $customProperty
```

Opção para usar proxy de sistema nos Citrix Cloud Connectors para tráfego de API GCP redirecionado

Para rotear todo o tráfego externo através de um proxy não transparente, configure a conexão do host com a propriedade personalizada `UseSystemProxyForHypervisorTrafficOnConnectors`. Isso redireciona o tráfego de internet da API GCP nos Citrix Cloud Connectors através do proxy do sistema. Siga os mesmos passos descritos em Habilitar o proxy para configurar a conexão do host com a propriedade personalizada. No entanto, certifique-se de anexar a configuração da propriedade `<Property xsi:type="StringProperty" Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />` ao `CustomProperties` para habilitar o proxy.

```
<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />
```

Exemplo:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

 <Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True"/>

 <Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
Value="True"/>

<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />

</CustomProperties>
```

Nota:

Depois de definir esta propriedade, o proxy configurado nas configurações `netsh winhttp` nos Citrix Cloud Connectors é usado para o tráfego de saída para o provedor de serviços em nuvem.

Especificar chave CMEK global e regional

> **Nota:**
>
> O suporte para CMEK no GCP está atualmente em Pré-visualização.

> Existem dois tipos de chaves de criptografia gerenciadas pelo cliente (CMEK) no GCP:

- Regional: Chaves de criptografia que só podem ser usadas por recursos na mesma região.
- Global: Chaves de criptografia que podem ser usadas por recursos de várias regiões.

Você pode navegar e usar chaves de criptografia gerenciadas pelo cliente (CMEK) globais ou regionais de todos os projetos acessíveis à conta de serviço. Você pode então usar a chave para criar um catálogo de máquinas MCS habilitado para CMEK e atualizar um catálogo de máquinas MCS habilitado para CMEK existente usando o comando `Set-ProvScheme`. Para obter informações sobre como criar um catálogo habilitado para CMEK usando PowerShell, consulte Criar um catálogo com CMEK usando propriedades personalizadas.

Para este recurso, você precisa de permissões adicionais para as duas contas de serviço a seguir:

- A conta de serviço do projeto atual com a qual a conexão de hospedagem é criada.
- O Agente de Serviço do Compute Engine do projeto atual (que tem o e-mail: `service-PROJECT_NUMBER@compute-system.iam.gserviceaccount.com`). Para obter mais informações, consulte Agente de Serviço do Compute Engine.

Nas contas de serviço, você deve atribuir as seguintes funções no projeto que possui as chaves criptográficas que você deseja usar (por exemplo, projeto compartilhado):

- Visualizador do Cloud KMS
- Criptografador/Descriptografador de Chave Criptográfica do Cloud KMS

Se você não atribuir às funções, certifique-se de ter as seguintes permissões:

- resourcemanager.projects.get
- cloudkms.keyRings.list
- cloudkms.keyRings.get
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list

- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

Listar as chaves de criptografia

Você pode listar as chaves de criptografia globais e regionais dentro do mesmo projeto e de todos os outros projetos acessíveis usando os comandos do PowerShell. Para fazer isso:

1. Abra uma janela do PowerShell a partir do host do Delivery Controller™ ou do PowerShell remoto.
2. Execute o comando `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando para listar as chaves de criptografia. Exemplo:
   - Para listar o conteúdo da pasta `encryptionKeys`:

     ```
     Get-ChildItem XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder
     ```

   - Para obter chaves de criptografia globais dentro do mesmo projeto:

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\myglobalkeyring.globalkeyring\mygl
     obalkey.cryptokey
     ```

   - Para obter chaves de criptografia regionais dentro do mesmo projeto:

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\regional-ring.keyring\shared-
     key.cryptokey
     ```

   - Para obter chaves de criptografia globais de outro projeto acessível (por exemplo: myanotherproject):

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\myanotherproject.project\shared-
     global-ring.globalkeyring\shared-key.cryptokey
     ```

- Para obter chaves de criptografia regionais de outro projeto acessível (por exemplo: myanotherproject):

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myanotherproject .project.project\
shared-uscentral.keyring\shared-uscentral-key.cryptokey
```

Nota:

- A extensão do item de inventário do conjunto de chaves para um conjunto de chaves global é `.globalkeyring`.
- O ID dos conjuntos de chaves globais contém a palavra `global`.

Permissões GCP necessárias

Esta seção contém a lista completa de permissões GCP. Use o conjunto completo de permissões conforme fornecido na seção para que a funcionalidade funcione corretamente.

Nota:

O GCP está introduzindo alterações no comportamento padrão e no uso de contas de serviço do Cloud Build Services após April 29, 2024. Para obter mais informações, consulte Alteração da Conta de Serviço do Cloud Build. Seus projetos Google existentes com a API Cloud Build ativada antes de April 29, 2024 não são afetados por esta alteração. No entanto, se você quiser ter o comportamento existente do Cloud Build Service após April 29, poderá criar ou aplicar a política da organização para desativar a imposição da restrição antes de ativar a API. Se você definir a nova política da organização, ainda poderá seguir as permissões existentes nesta seção e os itens que estão marcados como **Antes da Alteração da Conta de Serviço do Cloud Build**. Caso contrário, siga as permissões existentes e os itens que estão marcados como **Após a Alteração da Conta de Serviço do Cloud Build**.

Criando uma conexão de host

- Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento:

```
compute.instanceTemplates.list

compute.instances.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get
```

As seguintes funções definidas pelo Google possuem as permissões listadas acima:

- Administrador de Computação
- Usuário do Cloud Datastore

- Permissões adicionais necessárias para Shared VPC para a Conta de Serviço do Citrix Cloud no projeto Shared VPC:

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Usuário da Rede de Computação

- Nas contas de serviço, você deve atribuir as seguintes funções no projeto que possui as chaves criptográficas que você deseja usar (por exemplo, projeto compartilhado):

- Visualizador do Cloud KMS
- Criptografador/Descriptografador de Chave Criptográfica do Cloud KMS

Se você não atribuir às funções, certifique-se de ter as seguintes permissões:

- resourcemanager.projects.get
- cloudkms.keyRings.list
- cloudkms.keyRings.get
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

Gerenciamento de energia de VMs

Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento no caso de catálogos somente com gerenciamento de energia:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get
```

```
compute.zoneOperations.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Administrador de Computação
- Usuário do Cloud Datastore

Criar, atualizar ou excluir VMs

- Permissões mínimas necessárias para a Conta de Serviço do Citrix Cloud no projeto de Provisionamento:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create
```

```
compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset
```

```
compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels
```

```
compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

```
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Administrador de Computação
- Administrador de Armazenamento
- Editor do Cloud Build
- Usuário da Conta de Serviço
- Usuário do Cloud Datastore

- Permissões adicionais necessárias para VPC Compartilhada para a Conta de Serviço do Citrix Cloud no projeto de VPC Compartilhada para criar uma unidade de hospedagem usando VPC e sub-rede do projeto de VPC Compartilhada:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Usuário da Rede de Computação
- Usuário do Cloud Datastore

Permissões mínimas necessárias ao baixar o disco de instruções de preparação para o MCS:

- (Antes da alteração da conta de serviço do Cloud Build): Atribua essas permissões à conta de serviço do Cloud Build no projeto de provisionamento.

- (Após a alteração da conta de serviço do Cloud Build): Atribua essas permissões à conta de serviço do Cloud Compute no projeto de provisionamento.

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get
```

```
compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

  - Conta de Serviço do Cloud Build (Após a alteração da Conta de Serviço do Cloud Build, é a Conta de Serviço do Cloud Compute)
  - Administrador de Instância de Computação
  - Usuário da Conta de Serviço

- Permissões mínimas necessárias para a Conta de Serviço do Cloud Compute no projeto de provisionamento exigidas pelo serviço Google Cloud Build ao baixar o disco de instruções de preparação para o MCS:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

  As seguintes funções definidas pelo Google têm as permissões listadas acima:

  - Usuário da Rede de Computação
  - Usuário da Conta de Armazenamento
  - Usuário do Cloud Datastore

  Permissões adicionais necessárias para VPC Compartilhada ao baixar o disco de instruções de preparação para o MCS:

  - (Antes da alteração da conta de serviço do Cloud Build): Atribua estas permissões à conta de serviço do Cloud Build no projeto de provisionamento.
  - (Após a alteração da conta de serviço do Cloud Build): Atribua estas permissões à conta de serviço do Cloud Compute no projeto de provisionamento.

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list

compute.subnetworks.use
```

```
resourcemanager.projects.get
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Usuário da Rede de Computação
- Usuário da Conta de Armazenamento
- Usuário do Cloud Datastore

- Permissões adicionais necessárias para o Cloud Key Management Service (KMS) para a conta de serviço do Citrix Cloud no projeto de provisionamento:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

As seguintes funções definidas pelo Google têm as permissões listadas acima:

- Visualizador de KMS de Computação

Permissões gerais

A seguir estão as permissões para a conta de serviço do Citrix Cloud no projeto de provisionamento para todos os recursos suportados no MCS. Essas permissões fornecem a melhor compatibilidade daqui para frente:

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get
```

```
compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list
```

```
compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig
```

```
compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get
```

```
compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs

compute.resourcePolicies.use
```

```
cloudkms.cryptoKeyVersions.useToDecrypt

cloudkms.cryptoKeyVersions.useToEncrypt
```

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para informações específicas do Google Cloud Platform (GCP), consulte Criar um catálogo do Google Cloud Platform.

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização do Google Cloud.

Conexão com HPE Moonshot

(/pt-br/citrix-daas/install-configure/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos do HPE Moonshot.

> **Nota:**

> Antes de criar uma conexão com o HPE Moonshot, você precisa primeiro concluir a configuração da sua conta HPE. Consulte Ambientes de virtualização HPE Moonshot.

Criar uma conexão

Você pode criar uma conexão com o HPE Moonshot usando:

- Studio
- Comandos PowerShell

Criar uma conexão usando o Studio

1. Na página **Adicionar Conexão e Recursos**, selecione **HPE Moonshot** como o tipo de conexão.
2. Insira o endereço de conexão do seu Moonshot iLO Chassis Manager. Você pode usar um endereço IP, nome de host ou FQDN para o endereço.
3. Insira suas credenciais administrativas do chassi e um nome de conexão amigável.

A configuração da conexão é interrompida quando uma das seguintes situações ocorre:

- O DaaS recebe um certificado assinado por CA público com erros: Uma mensagem de erro aparece. Siga as instruções na tela para corrigir o problema. Caso contrário, você não poderá prosseguir com a criação da conexão.
- O DaaS recebe um certificado assinado por CA privado. Uma página de aviso aparece. Compare o thumbprint recebido com o do servidor para a validade do certificado. Se for válido, selecione **Confiar no certificado** e clique em **OK** para prosseguir com a criação da conexão. O DaaS então confiará no certificado e armazenará o thumbprint para validação futura.

Criar uma conexão usando comandos PowerShell

Ao criar uma conexão usando o comando PowerShell, forneça as seguintes informações:

- IP: Endereço IP do Servidor HPE
- Nome de usuário: Nome de usuário HPE
- Senha: Senha HPE

Por exemplo:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

> **Nota:**
>
> O parâmetro `sslthumbprint` é necessário apenas para certificados assinados por CA privada.

Validação de certificado e thumbprint

Para criar uma conexão bem-sucedida com o **HPE Moonshot**, o certificado não deve ter erros e o thumbprint deve ter um valor correto. A seguir estão os casos de uso relacionados à validação de certificado e thumbprint:

- O certificado assinado por CA pública tem erros. A conexão não é criada com sucesso. Consulte os detalhes do erro e resolva o problema.
- Certificado assinado por CA pública sem erros. A conexão é criada com sucesso, e o valor `SslThumbprints` é **Nulo**.
- Certificado assinado por CA privada sem erros e um valor `sslthumbprint`. A conexão é criada com sucesso com um valor `SslThumbprints` correto.
- Certificado assinado por CA privada com um valor de thumbprint incorreto. A conexão não é criada com sucesso.
- Certificado assinado por CA privada sem erros. A conexão é criada com sucesso. O `SSlThumbprints` é **Nulo** ao criar a conexão. O valor `SSlThumbprints` é atualizado para um valor pelo serviço do site.

Gerenciar conexões

Esta seção detalha como você pode gerenciar conexões:

- Corrigir problemas de certificado usando o Studio
- Atualizar o valor do thumbprint usando o comando PowerShell

Corrigir problemas de certificado

O DaaS bloqueia uma conexão HPE Moonshot quando surgem problemas de certificado, impedindo que você entregue e gerencie cargas de trabalho em nós HPE Moonshot associados. Você verá um ícone de erro ao lado da conexão na lista **Conexões de host**. Consulte a tabela a seguir para problemas e soluções específicas.

PROBLEMA	SOLUÇÃO
Ocorre um erro de certificado para o certificado público assinado por CA	Clique na conexão e selecione a guia **Solução de problemas**. Visualize os detalhes do erro e resolva o problema.
O certificado recebido é assinado por CA privada ou expirou.	Edite a conexão do host para atualizar o thumbprint do certificado. Etapas detalhadas:

PROBLEMA	SOLUÇÃO	
	1. Selecione a conexão e clique em **Editar Conexão**. 2. Na página **Propriedades da Conexão**, clique em **Editar configurações**. 3. Insira a senha para se conectar ao chassi HPE Moonshot e, em seguida, clique em **Salvar**. 4. Na página **Aviso** que aparece, compare a impressão digital recebida com a do servidor para validar o certificado. 5. Se forem iguais, selecione **Confiar no certificado** e, em seguida, clique em **OK**.	

Atualizar valores de impressão digital

Após criar a conexão, você pode atualizar o valor da impressão digital de uma conexão usando o comando PowerShell `Set-Item`. Por exemplo, execute os seguintes comandos:

1. Obtenha os detalhes da conexão de uma conexão. Por exemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. Atualize o valor da impressão digital. Por exemplo:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. Verifique o valor da impressão digital atualizado. Por exemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

Nota:

A atualização falha se você fornecer um valor de impressão digital incorreto no comando `Set-Item`.

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas sobre o HPE Moonshot, consulte Criar um catálogo de máquinas HPE Moonshot.

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização HPE Moonshot

Conexão com o Microsoft Azure Resource Manager

(/pt-br/citrix-daas/install-configure/connections.html) descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos para ambientes de nuvem do Azure Resource Manager.

Nota:

Antes de criar uma conexão com o Microsoft Azure, você deve concluir a configuração da sua conta do Azure como um local de recurso. Consulte Ambientes de virtualização do Microsoft Azure Resource Manager.

Criar entidades de serviço e conexões

Antes de criar conexões, você deve configurar entidades de serviço que as conexões usam para acessar recursos do Azure. Você pode criar uma conexão de duas maneiras:

- Criar uma entidade de serviço e uma conexão juntas usando o Studio
- Criar uma conexão usando uma entidade de serviço criada anteriormente

Esta seção mostra como concluir estas tarefas:

- Criar uma entidade de serviço e conexão usando o Studio
- Criar uma entidade de serviço usando o PowerShell
- Obter o segredo do aplicativo no Azure
- Criar uma conexão usando uma entidade de serviço existente

Considerações

Antes de começar, esteja ciente destas considerações:

- A Citrix® recomenda o uso de service principals com uma função de *Colaborador*. No entanto, consulte a seção Permissões Mínimas para obter a lista de permissões mínimas.
- Ao criar a primeira conexão, o Azure solicita que você conceda as permissões necessárias. Para futuras conexões, você ainda deve autenticar, mas o Azure se lembrará do seu consentimento anterior e não exibirá o prompt novamente.
- Depois de autenticar com o Azure pela primeira vez, um aplicativo multi-tenant de propriedade da Citrix (ID: `08b70dc3-76c5-4611-ba7d-3312ba36cb2b`) é convidado para o seu Microsoft Entra ID em nome da conta autenticada.
- As contas usadas para autenticação devem ter permissões para atribuir funções na assinatura usando o Azure RBAC. Exemplo: Proprietário, Administrador de Controle de Acesso Baseado em Função ou Administrador de Acesso de Usuário da assinatura.
- A conta usada para autenticação deve ser membro do diretório da assinatura. Existem dois tipos de contas a serem observados: 'Work or School' e 'personal Microsoft account'. Consulte CTX219211 para obter detalhes.
- Embora você possa usar uma conta Microsoft existente adicionando-a como membro do diretório da assinatura, podem ocorrer complicações se o usuário tiver recebido anteriormente acesso de convidado a um dos recursos do diretório. Nesse caso, ele pode ter uma entrada de espaço reservado no diretório que não concede as permissões necessárias, e um erro é retornado.

Corrija isso removendo os recursos do diretório e adicionando-os novamente explicitamente. No entanto, use esta opção com cuidado, pois ela pode ter efeitos indesejados em outros recursos que esta conta pode acessar.

- Existe um problema conhecido em que certas contas são detectadas como convidados do diretório quando na verdade são membros. Configurações como esta geralmente ocorrem com contas de diretório mais antigas e estabelecidas. Solução alternativa: adicione uma conta ao diretório, que assume o valor de associação adequado.
- Grupos de recursos são simplesmente contêineres para recursos, e eles podem conter recursos de regiões diferentes da sua própria região. Isso pode ser potencialmente confuso se você esperar que os recursos exibidos na região de um grupo de recursos estejam disponíveis.
- Certifique-se de que sua rede e sub-rede sejam grandes o suficiente para hospedar o número de máquinas que você precisa. Isso requer alguma previsão, mas a Microsoft ajuda você a especificar os valores corretos, com orientação sobre a capacidade do espaço de endereço.

Criar um service principal e uma conexão usando o Studio

> **Importante:**

> Este recurso ainda não está disponível para assinaturas do Azure China.

> Com o Studio, você pode criar um service principal e uma conexão em um único fluxo de trabalho. Os service principals concedem às conexões acesso aos recursos do Azure. Quando você autenticar no Azure para criar um service principal, um aplicativo é registrado no Azure. Uma chave secreta (chamada *client secret* ou *application secret*) é criada para o aplicativo registrado. O aplicativo registrado (uma *conexão* neste caso) usa o client secret para autenticar no Microsoft Entra ID.

Antes de começar, certifique-se de ter cumprido estes pré-requisitos:

- Você tem uma conta de usuário no locatário do Microsoft Entra da sua assinatura.
- As contas usadas para autenticação devem ter permissões para atribuir funções na assinatura usando o Azure RBAC. Exemplo: Proprietário, Administrador de Controle de Acesso Baseado em Função ou Administrador de Acesso de Usuário da assinatura.
- Você tem permissões de administrador global, administrador de aplicativo ou desenvolvedor de aplicativo para autenticação. As permissões podem ser revogadas depois de criar uma

conexão de host. Para obter mais informações sobre funções, consulte Funções internas do Microsoft Entra.

Use o assistente **Adicionar Conexão e Recursos** para criar um principal de serviço e uma conexão juntos:

1. Na página **Conexão**, selecione **Criar uma nova conexão**, o tipo de conexão **Microsoft Azure** e seu ambiente Azure.
2. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione **Avançar**.
3. Na página **Detalhes da Conexão**, selecione o modo de autenticação **Segredo do cliente do aplicativo**, crie um principal de serviço e defina o nome da conexão da seguinte forma:

    a. Insira seu ID de assinatura do Azure e um nome para a conexão. Depois de inserir o ID da assinatura, o botão **Criar novo** é ativado.

> **Nota:**
>
> O nome da conexão pode conter 1 a 64 caracteres e não pode conter apenas espaços em branco ou os caracteres `\/;:#.*?=<>|[]{}"'()'`.

    a. Selecione **Criar novo** e, em seguida, insira o nome de usuário e a senha da conta do Microsoft Entra.
    b. Selecione **Entrar**.
    c. Selecione **Aceitar** para conceder ao Citrix DaaS™ as permissões listadas. O Azure cria um principal de serviço que permite ao Citrix DaaS gerenciar recursos do Azure em nome do usuário especificado.

> **Nota:**
>
> O Citrix DaaS requer as seguintes permissões para criar um novo principal de serviço:
>
> - **Acessar o Gerenciamento de Serviços do Azure como você**
> - **Ler e gravar aplicativos**

- **Fazer login e ler seu perfil**
- **Manter o acesso aos dados aos quais você concedeu acesso**

d. Depois de selecionar **Aceitar**, você será levado de volta para a página **Detalhes da Conexão**.

Observação:

Depois de autenticar com sucesso no Azure, os botões **Criar novo** e **Usar existente** desaparecem. O texto **Conexão bem-sucedida** aparece com uma marca de seleção verde, indicando a conexão bem-sucedida à sua assinatura do Azure.

e. Para rotear solicitações de API para o Azure por meio dos Citrix Cloud™ Connectors, marque a caixa de seleção **Roteie o tráfego por meio dos Citrix Cloud Connectors**. Quando os Cloud Connectors não têm acesso direto à Internet, você pode selecionar **Usar o proxy configurado nos Citrix Cloud Connectors** para garantir que a conectividade do Azure funcione corretamente por meio dos Citrix Cloud Connectors.

Alternativamente, você pode habilitar esse recurso usando o PowerShell. Para obter mais informações, consulte Criar um ambiente seguro para tráfego gerenciado pelo Azure.

Observação:

Esta opção está disponível apenas quando há Citrix Cloud Connectors ativos em sua implantação. Atualmente, esse recurso não é compatível com Connector Appliances.

f. Selecione **Avançar**.

Observação:

Você não pode prosseguir para a próxima página até que autenticar com sucesso no Azure e consinta em conceder as permissões necessárias.

4. Configure os recursos para a conexão da seguinte forma:

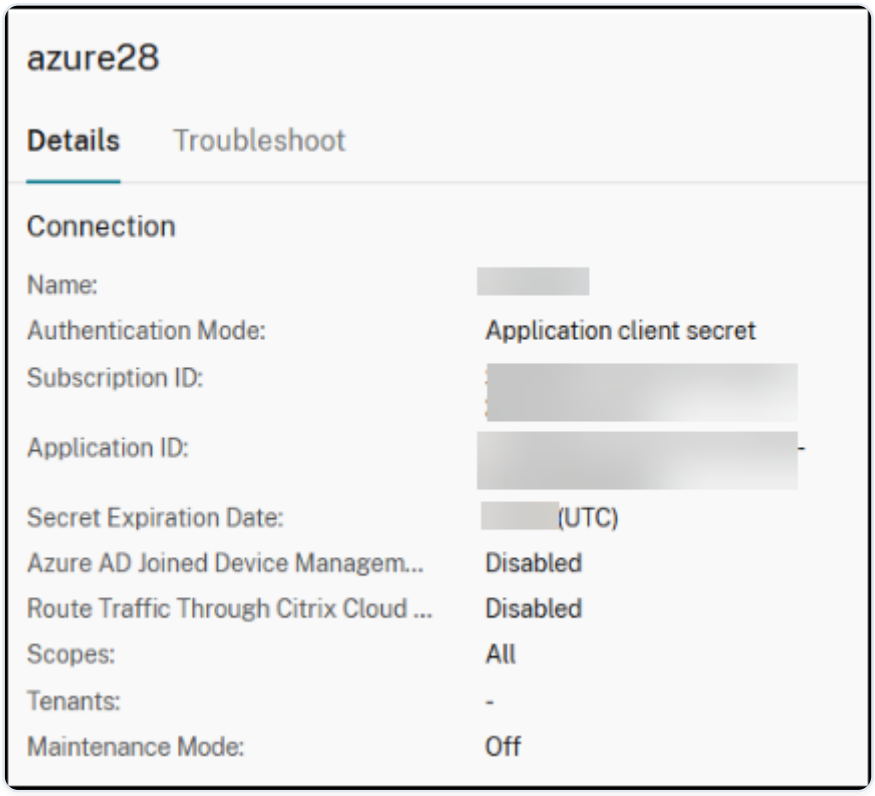
- Na página **Região**, selecione uma região.
- Na página **Rede**, faça o seguinte:
  - Digite um nome de recurso de 1 a 64 caracteres para ajudar a identificar a combinação de região e rede. Um nome de recurso não pode conter apenas espaços em branco ou os caracteres `\/;:#.*?=<>|[]{}"'()'`.
  - Selecione um par de rede virtual/grupo de recursos. (Se você tiver mais de uma rede virtual com o mesmo nome, o emparelhamento do nome da rede com o grupo de recursos fornece combinações exclusivas.) Se a região selecionada na página anterior não tiver nenhuma rede virtual, retorne a essa página e selecione uma região que tenha redes virtuais.

5. Na página **Resumo**, visualize um resumo das configurações e selecione **Concluir** para finalizar a configuração.

VISUALIZAR O ID DO APLICATIVO

Depois de criar uma conexão, você pode visualizar o ID do aplicativo que a conexão usa para acessar os recursos do Azure.

Na lista **Conexão e Recursos**, selecione a conexão para visualizar os detalhes. A guia **Detalhes** mostra o ID do Aplicativo.



Criar um principal de serviço usando PowerShell

Para criar um principal de serviço usando PowerShell, conecte-se à sua assinatura do Azure Resource Manager e use os cmdlets do PowerShell fornecidos nas seções a seguir.

Certifique-se de ter estes itens prontos:

- **SubscriptionId:** `SubscriptionID` do Azure Resource Manager para a assinatura onde você deseja provisionar VDAs.
- **ActiveDirectoryID**: ID do locatário do aplicativo que você registrou com o Microsoft Entra ID.
- **ApplicationName:** Nome para o aplicativo a ser criado no Microsoft Entra ID.

As etapas detalhadas são as seguintes:

1. Conecte-se à sua assinatura do Azure Resource Manager.

   ```
   Connect-AzAccount
   ```

2. Selecione a assinatura do Azure Resource Manager onde você deseja criar a entidade de serviço.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

3. Crie o aplicativo em seu locatário do AD.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

4. Crie uma entidade de serviço.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

5. Atribua uma função à entidade de serviço.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
   $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

6. Na janela de saída do console do PowerShell, anote o ApplicationId. Você fornece esse ID ao criar a conexão de host.

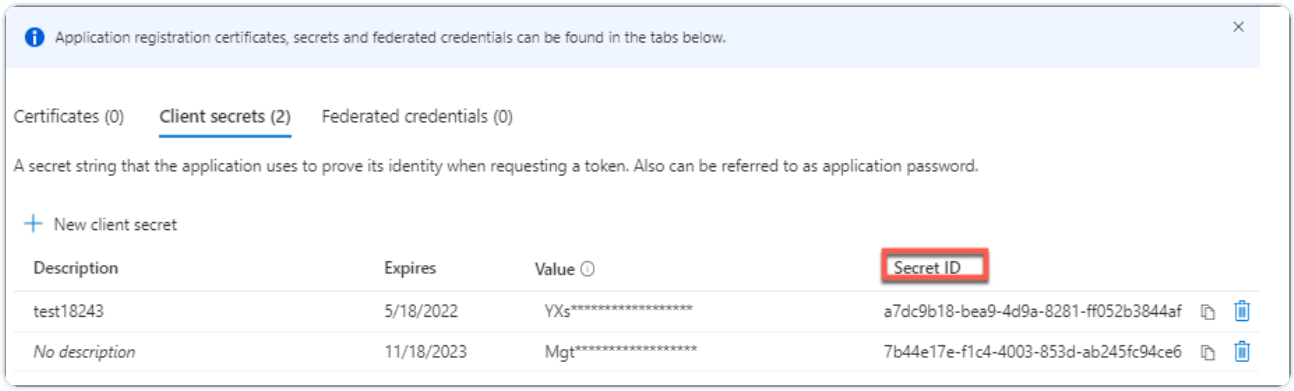
Obtenha o segredo do aplicativo no Azure

Para criar uma conexão usando uma entidade de serviço existente, você deve primeiro obter o ID do aplicativo e o segredo da entidade de serviço no portal do Azure.

As etapas detalhadas são as seguintes:

1. Obtenha o **ID do Aplicativo** no Studio ou usando o PowerShell.

2. Faça login no portal do Azure.
3. No Azure, selecione **Microsoft Entra ID**.
4. Em **Registros de aplicativo** no Microsoft Entra ID, selecione seu aplicativo.
5. Vá para **Certificados e segredos**.
6. Clique em **Segredos do cliente**.



Criar uma conexão usando uma entidade de serviço existente

Se você já tiver uma entidade de serviço, poderá usá-la para criar uma conexão usando o Studio.

Certifique-se de ter estes itens prontos:

- SubscriptionId
- ActiveDirectoryID (ID do locatário)
- ID do Aplicativo
- Segredo do aplicativo

  Para obter mais informações, consulte Obter o segredo do aplicativo.
- Data de expiração do segredo

As etapas detalhadas são as seguintes:

No assistente **Adicionar Conexão e Recursos**:

1. Na página **Conexão**, selecione **Criar uma nova conexão**, o tipo de conexão **Microsoft Azure** e seu ambiente Azure.
2. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione **Avançar**.
3. Na página **Detalhes da Conexão**, selecione o modo de autenticação **Segredo do cliente do aplicativo**, em seguida, insira seu ID de assinatura do Azure e um nome para a conexão.

> **Nota:**
>
> O nome da conexão pode conter de 1 a 64 caracteres e não pode conter apenas espaços em branco ou os caracteres `\/;:#.*?=<>|[]{}"'()'`.

4. Selecione **Usar existente**. Na janela **Detalhes do Principal de Serviço Existente**, insira as seguintes configurações para o principal de serviço existente. Depois de inserir os detalhes, o botão **Salvar** é ativado. Selecione **Salvar**. Você não pode prosseguir além desta página até fornecer detalhes válidos.

   - **ID da Assinatura**. Insira seu ID de assinatura do Azure. Para obter seu ID de assinatura, faça login no portal do Azure e navegar para **Assinaturas > Visão geral**.
   - **ID do Active Directory** (ID do locatário). Insira o ID do Diretório (locatário) do aplicativo que você registrou com o Microsoft Entra ID.
   - **ID do Aplicativo**. Insira o ID do Aplicativo (cliente) do aplicativo que você registrou com o Microsoft Entra ID.
   - **Segredo do aplicativo**. Insira uma chave secreta (segredo do cliente). O aplicativo registrado usa a chave para autenticar no Microsoft Entra ID. Recomendamos que você altere as chaves regularmente por motivos de segurança. Certifique-se de salvar a chave, pois você não poderá recuperá-la mais tarde.
   - **Data de expiração do segredo**. Insira a data após a qual o segredo do aplicativo expira. Você receberá um alerta no console a partir de 14 dias antes da expiração da chave secreta. No entanto, se a chave secreta expirar, você receberá erros.

     > **Nota:**
     >
     > Para fins de segurança, o período de expiração não pode ser superior a dois anos a partir de agora.

   - **URL de autenticação**. Este campo é preenchido automaticamente e não é editável.
   - **URL de gerenciamento**. Este campo é preenchido automaticamente e não é editável.
   - **Sufixo de armazenamento**. Este campo é preenchido automaticamente e não é editável.
   - **Endpoint de armazenamento de blobs do Azure para upload ou download de discos ou snapshots**. Este campo é preenchido automaticamente e não é editável.

- **Serviço Key Vault**. Este campo é preenchido automaticamente e não é editável.
- **Sufixo do barramento de serviço**. Este campo é preenchido automaticamente e não é editável.

  O acesso aos seguintes endpoints é necessário para criar um catálogo MCS no Azure. O acesso a esses endpoints otimiza a conectividade entre sua rede e o portal do Azure e seus serviços.

  - URL de autenticação: `https://login.microsoftonline.com`
  - URL de gerenciamento: `https://management.azure.com`. Esta é uma URL de solicitação para APIs do provedor do Azure Resource Manager. O endpoint para gerenciamento depende do ambiente. Por exemplo, para o Azure Global, é `https://management.azure.com`, e para o Azure US Government, é `https://management.usgovcloudapi.net`.
  - Sufixo de armazenamento: `https://*.core.windows.net`. Este (*) é um caractere curinga para sufixo de armazenamento. Por exemplo, `https://demo.table.core.windows.net`.
  - Endpoint de armazenamento de blobs do Azure para upload ou download de discos ou snapshots: `https://*.storage.azure.net`. Este (*) é um caractere curinga para operações de importação e exportação de armazenamento de blobs. Por exemplo, `https://md-impexp-xxxxx.z[00-50].blob.storage.azure.net`.
  - Serviço Key Vault: `https://*.vault.azure.net`. Este (*) é um caractere curinga para o nome do cofre de chaves. Por exemplo, `https://<your-key-vault-name>.vault.azure.net`.
  - Sufixo do barramento de serviço: `https://*.servicebus.windows.net`. Este (*) é um caractere curinga para namespaces criados na nuvem global do Azure. Por exemplo, `https://{serviceNamespace}.servicebus.windows.net/{path}`.

5. Após selecionar **Salvar**, você será redirecionado para a página **Detalhes da Conexão**. Selecione **Avançar** para prosseguir para a próxima página.
6. Configure os recursos para a conexão da seguinte forma:

   - Na página **Região**, selecione uma região.
   - Na página **Rede**, faça o seguinte:

- Digite um nome de recurso de 1 a 64 caracteres para ajudar a identificar a combinação de região e rede. Um nome de recurso não pode conter apenas espaços em branco ou os caracteres `\/;:#.*?=<>|[]{}"'()'`.
- Selecione um par de rede virtual/grupo de recursos. (Se você tiver mais de uma rede virtual com o mesmo nome, o emparelhamento do nome da rede com o grupo de recursos fornece combinações exclusivas.) Se a região selecionada na página anterior não tiver nenhuma rede virtual, retorne a essa página e selecione uma região que tenha redes virtuais.

7. Na página **Resumo**, visualize um resumo das configurações e selecione **Concluir** para finalizar a configuração.

Gerenciar entidades de serviço e conexões

Esta seção detalha como você pode gerenciar entidades de serviço e conexões:

- Configurar as configurações de limitação do Azure
- Gerenciar a entidade de serviço de uma conexão de hospedagem existente
- Habilitar o compartilhamento de imagens no Azure
- Adicionar locatários compartilhados a uma conexão usando o Studio
- Implementar o compartilhamento de imagens usando o PowerShell
- Criar um ambiente seguro para o tráfego gerenciado pelo Azure
- Gerenciar o segredo do aplicativo e a data de expiração do segredo

Configurar as definições de limitação do Azure

O Azure Resource Manager limita as solicitações para assinaturas e locatários, roteando o tráfego com base em limites definidos, adaptados às necessidades específicas do provedor. Consulte Limitação de solicitações do Resource Manager no site da Microsoft para obter mais informações. Existem limites para assinaturas e locatários, onde o gerenciamento de muitas máquinas pode se tornar problemático. Por exemplo, uma assinatura que contém muitas máquinas pode apresentar problemas de desempenho relacionados a operações de energia.

> **Dica:**

> Para obter mais informações, consulte Melhorando o desempenho do Azure com o Machine Creation Services.

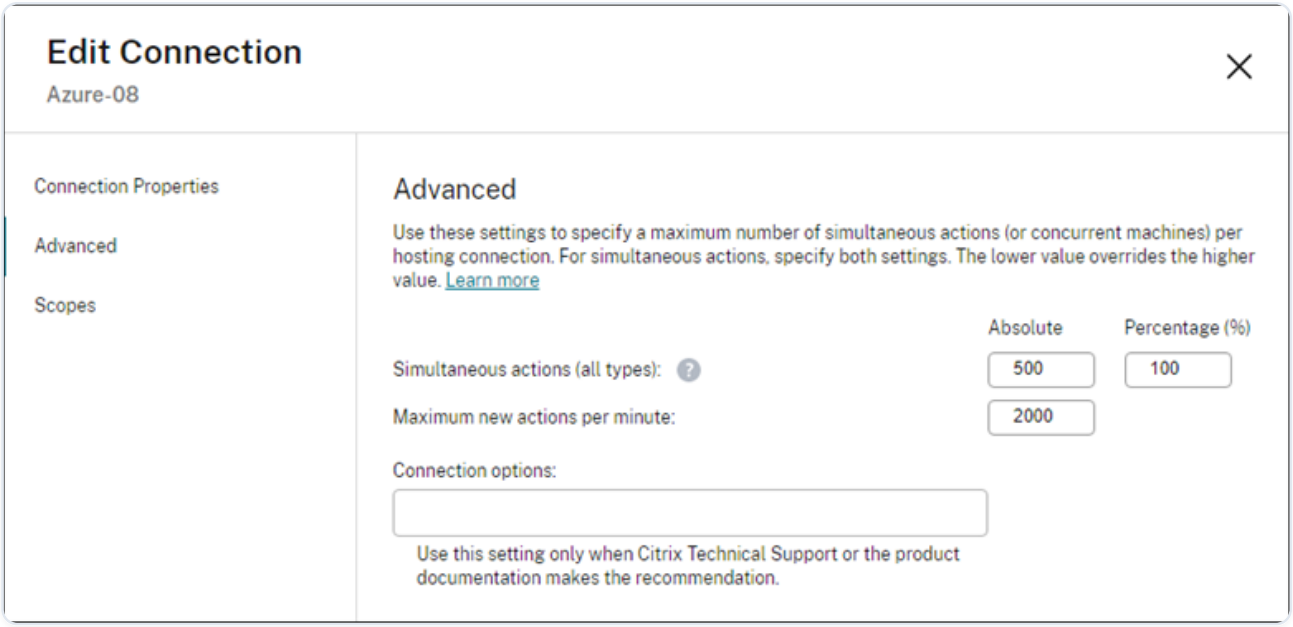
> Para ajudar a mitigar esses problemas, o Citrix DaaS permite remover a limitação interna do MCS para usar mais da cota de solicitação disponível do Azure.

Recomendamos as seguintes configurações ideais ao ligar ou desligar VMs em grandes assinaturas, por exemplo, aquelas que contêm 1.000 VMs:

- Operações simultâneas absolutas: 500
- Máximo de novas operações por minuto: 2000
- Concorrência máxima de operações: 500

Use o Studio para configurar as operações do Azure para uma determinada conexão de host:

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione uma conexão relacionada ao Azure para editá-la.
3. No assistente **Editar Conexão**, selecione **Avançado**.
4. Na página **Avançado**, use as opções de configuração para especificar o número de ações simultâneas e o máximo de novas ações por minuto, e quaisquer opções de conexão adicionais.



O MCS suporta um máximo de 500 operações simultâneas por padrão. Alternativamente, você pode usar o SDK do PowerShell Remoto para definir o número máximo de operações simultâneas.

Use a propriedade **PowerShell**, `MaximumConcurrentProvisioningOperations`, para especificar o número máximo de operações de provisionamento simultâneas do Azure. Ao usar esta propriedade, considere:

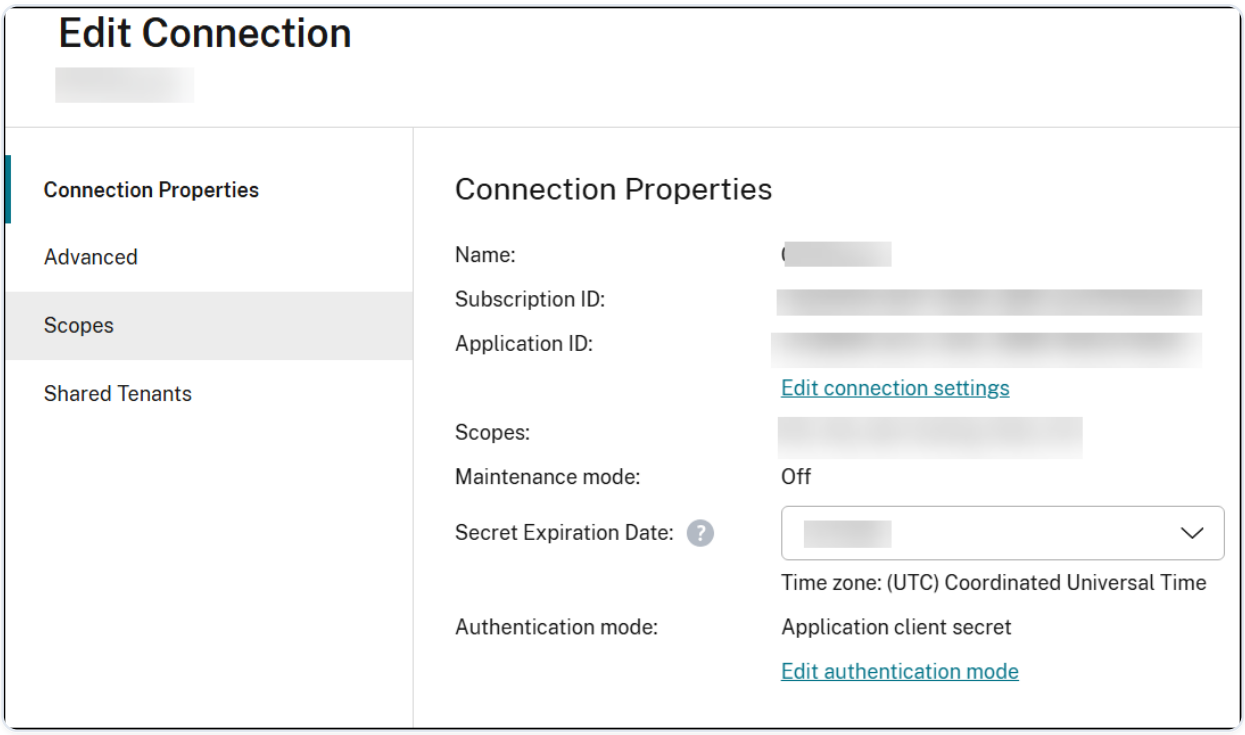
- O valor padrão de `MaximumConcurrentProvisioningOperations` é 500.
- Configure o parâmetro `MaximumConcurrentProvisioningOperations` usando o comando PowerShell `Set-item`.

Gerenciar o principal de serviço de uma conexão de hospedagem existente

Depois de criar uma conexão de hospedagem usando um principal de serviço, você pode optar por editar a conexão de hospedagem para ter:

- Novo principal de serviço
- Usar outro principal de serviço existente

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e, em seguida, selecione **Editar Conexão** na barra de ações.
3. Selecione **Propriedades da Conexão** no painel esquerdo.
4. Na página **Propriedades da Conexão** que aparece, clique em **Editar configurações de conexão**. Agora você pode optar por criar um novo principal de serviço ou usar outro principal de serviço existente.



- Clique em **Criar principal de serviço** para criar um novo principal de serviço. Siga as instruções para fazer login em sua conta de usuário do Microsoft Entra. A Citrix usa o ID de aplicativo multi-tenant `08b70dc3-76c5-4611-ba7d-3312ba36cb2b` para criar um novo principal de serviço para a conexão de host existente e conceder as permissões adequadas.

- Clique em **Usar existente** para usar outro principal de serviço existente para essa conexão de hospedagem.

Habilitar o compartilhamento de imagens no Azure

Ao criar ou atualizar catálogos de máquinas, você pode selecionar imagens compartilhadas de diferentes locatários e assinaturas do Azure (compartilhadas por meio da Galeria de Computação do Azure). Para habilitar o compartilhamento de imagens dentro ou entre locatários, você deve fazer as configurações necessárias no Azure:

- Compartilhar imagens dentro de um locatário (entre assinaturas)
- Compartilhar imagens entre locatários

COMPARTILHAR IMAGENS DENTRO DE UM LOCATÁRIO (ENTRE ASSINATURAS)

Para selecionar uma imagem na Galeria de Computação do Azure que pertence a uma assinatura diferente, a imagem deve ser compartilhada com o principal de serviço (SPN) dessa assinatura.

Por exemplo, se houver um principal de serviço (SPN 1), que está configurado no Studio como:

Principal de serviço: SPN 1

Assinatura: assinatura 1

Locatário: locatário 1

A imagem está em uma assinatura diferente, que está configurada no Studio como:

Assinatura: assinatura 2

Locatário: locatário 1

Se você quiser compartilhar a imagem na assinatura 2 com a assinatura 1 (SPN 1), vá para a assinatura 2 e compartilhe o grupo de recursos com o SPN1.

A imagem deve ser compartilhada com outro SPN usando o controle de acesso baseado em função do Azure (RBAC). O RBAC do Azure é o sistema de autorização usado para gerenciar o acesso aos recursos do Azure. Para obter mais informações sobre o RBAC do Azure, consulte o documento da Microsoft O que é o controle de acesso baseado em função do Azure (RBAC do Azure). Para conceder acesso, você atribui funções a principais de serviço no escopo do grupo de recursos com a função de Colaborador. Para atribuir funções do Azure, você deve ter a permissão `Microsoft.Authorization/roleAssignments/write`, como Administrador de Acesso do Usuário ou Proprietário. Para obter mais informações sobre como compartilhar imagens com outro SPN, consulte o documento da Microsoft Atribuir funções do Azure usando o portal do Azure.

COMPARTILHAR IMAGENS ENTRE LOCATÁRIOS

Para compartilhar imagens entre locatários com o Azure Compute Gallery, crie ou atualize o registro do aplicativo e use este aplicativo para criar a conexão de hospedagem.

Por exemplo, se houver dois locatários (Locatário 1 e Locatário 2) e você quiser compartilhar sua galeria de imagens com o Locatário 1, então:

1. Crie um registro de aplicativo para o Locatário 1. Para obter mais informações, consulte Criar o registro do aplicativo.
2. Conceda ao Locatário 2 acesso ao aplicativo solicitando um login usando um navegador. Substitua `Tenant2 ID` pelo ID do locatário do Locatário 1. Substitua `Application (client) ID` pelo ID do aplicativo do registro do aplicativo que você criou. Ao concluir as substituições, cole o URL em um navegador e siga os prompts de login para entrar no Locatário 2. Por exemplo:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   Para obter mais informações, consulte Conceder acesso ao Locatário 2.
3. Conceda ao aplicativo acesso ao grupo de recursos do Locatário 2. Faça login como Locatário 2 e conceda ao registro do aplicativo acesso ao grupo de recursos que contém a imagem da galeria. Para obter mais informações, consulte autenticar requests across tenants.

Adicionar locatários compartilhados a uma conexão usando o Studio

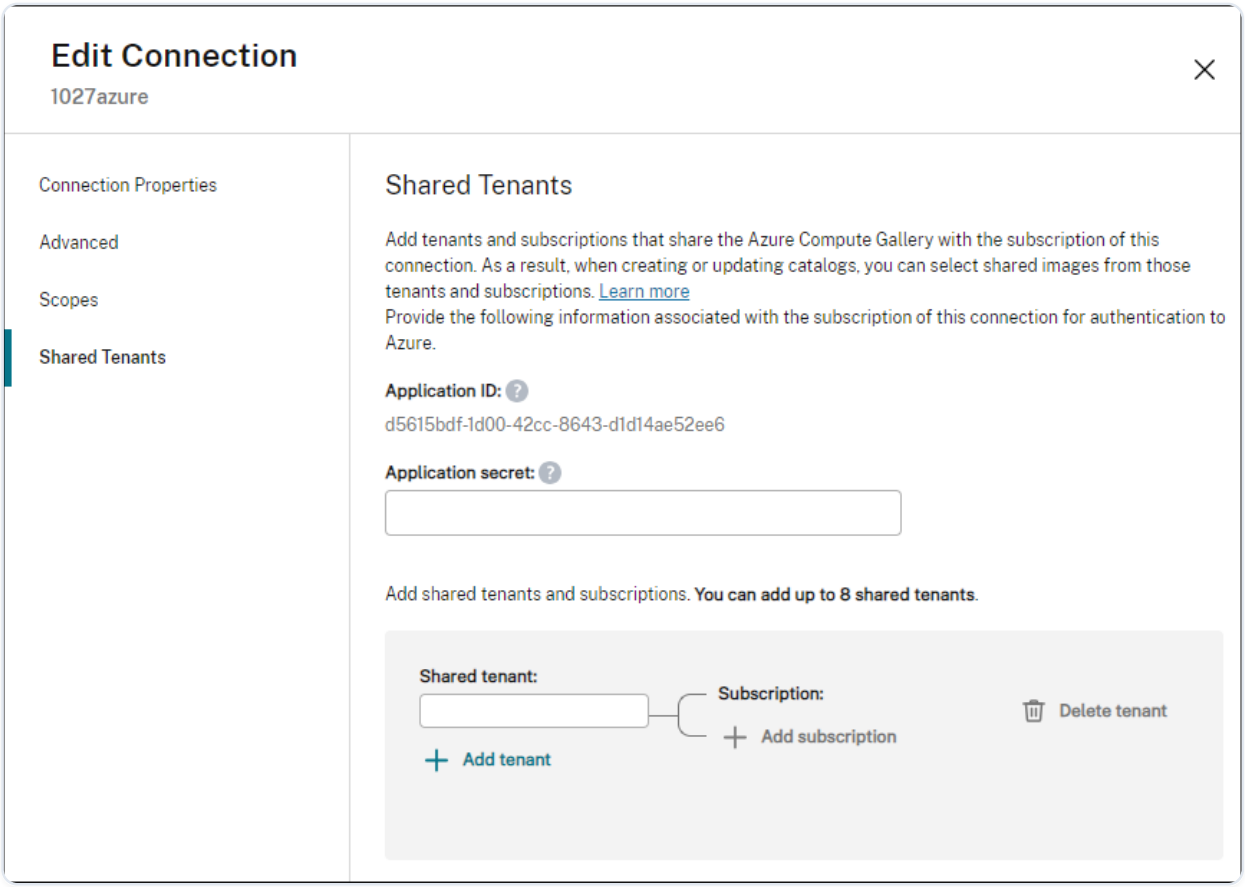
Ao criar ou atualizar catálogos de máquinas no Studio, você pode selecionar imagens compartilhadas de diferentes locatários e assinaturas do Azure (compartilhadas através do Azure Compute Gallery). O recurso exige que você forneça informações de locatário e assinatura compartilhados para as conexões de host associadas.

> **Nota:**

> Certifique-se de ter configurado as configurações necessárias no Azure para habilitar o compartilhamento de imagens entre locatários. Para obter mais informações, consulte Compartilhar imagens entre locatários.

> Conclua as seguintes etapas para uma conexão:

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e, em seguida, selecione **Editar Conexão** na barra de ações.



3. Em **Locatários Compartilhados**, faça o seguinte:
   a. Forneça o ID do aplicativo e o segredo do aplicativo associados à assinatura da conexão. O DaaS usa essas informações para autenticar no Microsoft Entra ID.
   b. Adicione locatários e assinaturas que compartilham a Galeria de Computação do Azure com a assinatura da conexão. Você pode adicionar até oito locatários compartilhados e oito assinaturas para cada locatário.
4. Quando terminar, selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Implementar o compartilhamento de imagens usando o PowerShell

Esta seção o orienta pelos processos de compartilhamento de imagens usando o PowerShell:

- Selecionar uma imagem de uma assinatura diferente
- Atualizar propriedades personalizadas de conexão de hospedagem com IDs de locatário compartilhados
- Selecionar uma imagem de um locatário diferente

SELECIONAR UMA IMAGEM DE UMA ASSINATURA DIFERENTE

Você pode selecionar uma imagem na Galeria de Computação do Azure que pertence a uma assinatura compartilhada diferente no mesmo locatário do Azure para criar e atualizar catálogos MCS usando comandos do PowerShell.

1. Na pasta raiz da unidade de hospedagem, o Citrix cria uma nova pasta de assinatura compartilhada chamada `sharedsubscription`.
2. Liste todas as assinaturas compartilhadas em um locatário.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. Selecione uma assinatura compartilhada e, em seguida, liste todos os grupos de recursos compartilhados dessa assinatura compartilhada.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. Selecione um grupo de recursos e, em seguida, liste todas as galerias desse grupo de recursos.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. Selecione uma galeria e, em seguida, liste todas as definições de imagem dessa galeria.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. Selecione uma definição de imagem e, em seguida, liste todas as versões de imagem dessa definição de imagem.

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. Crie e atualize um catálogo MCS usando os seguintes elementos:

    - Grupo de recursos
    - Galeria
    - Definição de imagem da galeria
    - Versão da imagem da galeria

ATUALIZAR PROPRIEDADES PERSONALIZADAS DE CONEXÃO DE HOSPEDAGEM COM IDS DE LOCATÁRIO COMPARTILHADAS

Use `Set-Item` para atualizar as propriedades personalizadas da conexão de hospedagem com IDs de locatário e IDs de assinatura compartilhadas. Adicione uma propriedade `SharedTenants` em `CustomProperties`. O formato de `Shared Tenants` é:

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

Por exemplo:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />
```

```
</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

Nota:

Você pode adicionar mais de um locatário. Cada locatário pode ter mais de uma assinatura.

SELECIONE UMA IMAGEM DE UM LOCATÁRIO DIFERENTE

Você pode selecionar uma imagem na Galeria de Computação do Azure que pertence a um locatário diferente do Azure para criar e atualizar catálogos MCS usando comandos do PowerShell.

1. Na pasta raiz da unidade de hospedagem, a Citrix cria uma nova pasta de assinatura compartilhada chamada `sharedsubscription`.
2. Listar todas as assinaturas compartilhadas.

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. Selecione uma assinatura compartilhada e, em seguida, liste todos os grupos de recursos compartilhados dessa assinatura compartilhada.

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription
   ```

4. Selecione um grupo de recursos e, em seguida, liste todas as galerias desse grupo de recursos.

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription\
   xyz.resourcegroup
   ```

5. Selecione uma galeria e, em seguida, liste todas as definições de imagem dessa galeria.

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery
```

6. Selecione uma definição de imagem e, em seguida, liste todas as versões de imagem dessa definição de imagem.

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. Crie e atualize um catálogo MCS usando os seguintes elementos:

   - Grupo de recursos
   - Galeria
   - Definição de imagem da galeria
   - Versão da imagem da galeria

Crie um ambiente seguro para o tráfego gerenciado pelo Azure

O MCS permite que o tráfego de rede (chamadas de API do Citrix Cloud para o hipervisor do Azure) seja roteado por meio de Cloud Connectors em seu ambiente. Essa implementação ajuda você a bloquear sua assinatura do Azure para permitir o tráfego de rede de endereços IP específicos. Para fazer isso, adicione `ProxyHypervisorTrafficThroughConnector` em `CustomProperties`. Depois de definir as propriedades personalizadas, você pode configurar políticas do Azure para ter acesso privado a discos gerenciados do Azure.

Se você configurar a política do Azure para criar Acessos de Disco automaticamente para cada novo disco usar pontos de extremidade privados, não poderá carregar ou baixar mais de cinco discos ou instantâneos ao mesmo tempo com o mesmo objeto de acesso a disco, conforme imposto pelo Azure. Esse limite é para cada catálogo de máquinas se você configurar a política do Azure no nível do grupo de recursos, e para todos os catálogos de máquinas se você configurar a política do Azure no nível da assinatura. Se você não configurar a política do Azure para criar Acessos de Disco automaticamente para cada novo disco usar pontos de extremidade privados, o limite de cinco operações simultâneas não será imposto.

> **Nota:**

> Atualmente, este recurso não é compatível com o Connector Appliance. Para limitações do Azure relacionadas a este recurso, consulte Restringir o acesso de importação/exportação para discos gerenciados usando o Azure Private Link.

HABILITAR O PROXY

Para habilitar o proxy, defina as propriedades personalizadas da seguinte forma na conexão do host:

1. Abra uma janela do PowerShell usando o SDK do PowerShell Remoto. Para obter mais informações, consulte `<https://docs.citrix.com/pt-br/citrix-daas/sdk-api.html#citrix-virtual-apps-and-desktops-remote-powershell-sdk/>`.
2. Execute os seguintes comandos:

```
Add-PSSnapin citrix*.

cd XDHyp:\Connections\

dir
```

3. Copie o `CustomProperties` da conexão para um bloco de notas e anexe a configuração de propriedade `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector" Value="True" />` ao `CustomProperties` para habilitar o proxy. Por exemplo:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty" Name="SubscriptionId"
Value="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />

<Property xsi:type="StringProperty" Name="ManagementEndpoint"
Value="https://management.azure.com/" />

<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
Value="https://login.microsoftonline.com/" />

<Property xsi:type="StringProperty" Name="StorageSuffix"
Value="core.windows.net" />

<Property xsi:type="StringProperty" Name="TenantId"
```

```
Value="5cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx" />

<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True" />

</CustomProperties>
```

4. Na janela do PowerShell, atribua uma variável às propriedades personalizadas modificadas. Por exemplo:

```
$customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation">

<Property xsi:type="StringProperty" Name="SubscriptionId"
Value="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />

<Property xsi:type="StringProperty" Name="ManagementEndpoint"
Value="https://management.azure.com/" />

<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
Value="https://login.microsoftonline.com/" />

<Property xsi:type="StringProperty" Name="StorageSuffix"
Value="core.windows.net" />

<Property xsi:type="StringProperty" Name="TenantId"
Value="5cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx" />

<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True" />

</CustomProperties>'
```

5. Execute `$cred = Get-Credential`. Se solicitado, forneça as credenciais de conexão. As credenciais são ID do Aplicativo Azure e segredo.
6. Execute `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password`.

> **Importante:**
>
> Se você receber uma mensagem informando que `SubscriptionId` está faltando, substitua todas as aspas duplas (“) por um acento grave seguido de aspas duplas (`”) na propriedade personalizada. Por exemplo:

```
<CustomProperties xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`" xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`"
Value=`"5cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx`" />

<Property xsi:type=`"StringProperty`"
Name=`"ProxyHypervisorTrafficThroughConnector`" Value=`"True`" />

</CustomProperties>
```

7. Execute `dir` para verificar as configurações atualizadas de `CustomProperties`.

Opção para usar proxy de sistema nos Citrix Cloud Connectors para tráfego de API do Azure redirecionado

Para rotear todo o tráfego externo através de um proxy não transparente, configure a conexão do host com a propriedade personalizada `UseSystemProxyForHypervisorTrafficOnConnectors`. Isso redireciona o tráfego de internet da API do Azure nos Citrix Cloud Connectors através do proxy do sistema.

Siga os mesmos passos descritos em Habilitar o proxy para configurar a conexão do host com a propriedade personalizada. No entanto, certifique-se de anexar a configuração de propriedade `<Property xsi:type="StringProperty" Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />` ao `CustomProperties` para habilitar o proxy.

```
<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />
```

Exemplo:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty" Name="SubscriptionId"
Value="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />

<Property xsi:type="StringProperty" Name="ManagementEndpoint"
Value="https://management.azure.com/" />

<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
Value="https://login.microsoftonline.com/" />

<Property xsi:type="StringProperty" Name="StorageSuffix"
Value="core.windows.net" />

<Property xsi:type="StringProperty" Name="TenantId"
Value="5cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx" />

<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True" />

<Property xsi:type="StringProperty"
Name="UseSystemProxyForHypervisorTrafficOnConnectors" Value="True" />

</CustomProperties>
```

Nota:

> Depois de definir esta propriedade, o proxy configurado nas configurações `netsh winhttp` nos Citrix Cloud Connectors é usado para tráfego de saída para o provedor de serviços em nuvem.

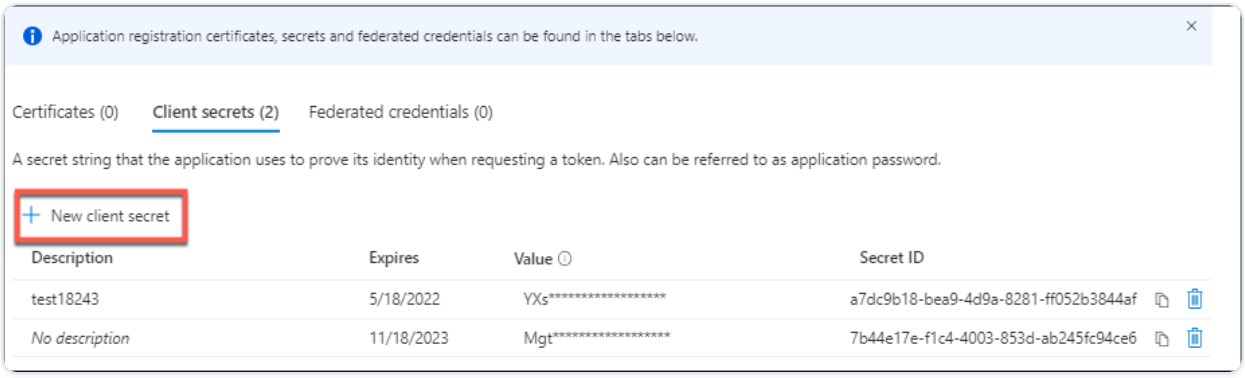
Gerenciar o segredo do aplicativo e a data de expiração do segredo

Certifique-se de alterar o segredo do aplicativo para uma conexão antes que o segredo expire. Você receberá um alerta no Studio antes que a chave secreta expire.

CRIAR UM SEGREDO DE APLICATIVO NO AZURE

Você pode criar um segredo de aplicativo para uma conexão através do portal do Azure.

1. Selecione **Microsoft Entra ID**.
2. Em **Registros de aplicativo** no Microsoft Entra ID, selecione seu aplicativo.
3. Vá para **Certificados e segredos**.
4. Clique em **Segredos do cliente > Novo segredo do cliente**.



5. Forneça uma descrição do segredo e especifique uma duração. Quando terminar, selecione **Adicionar**.

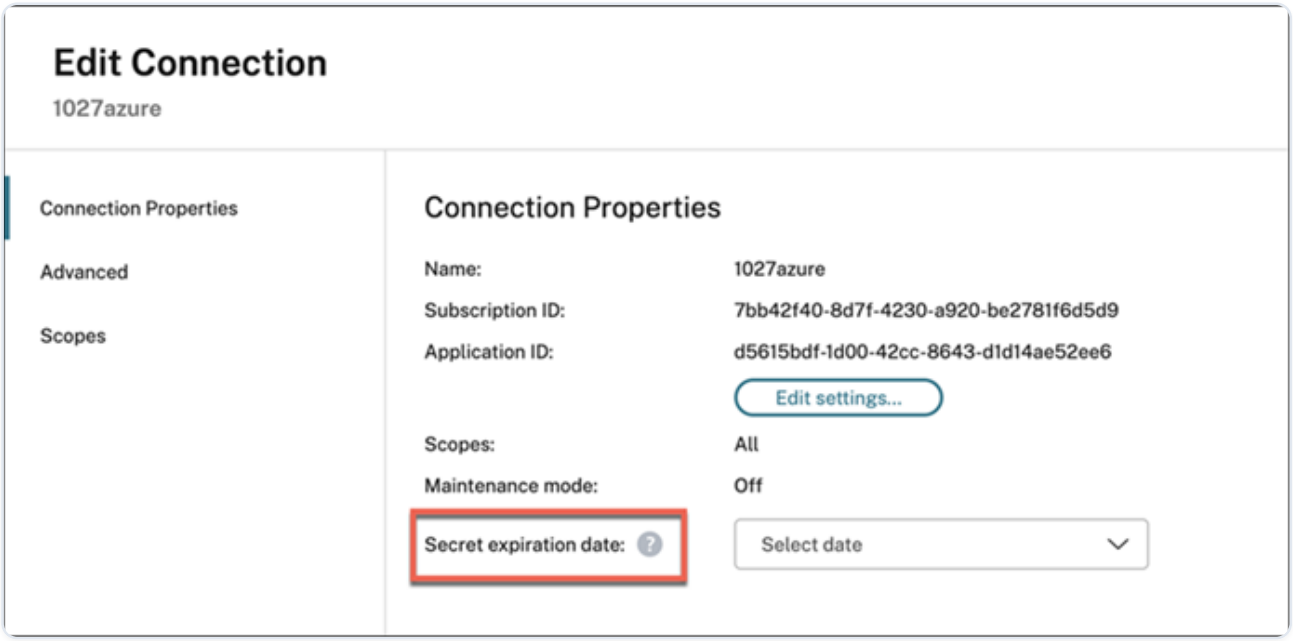
> **Nota:**
>
> Certifique-se de salvar o segredo do cliente, pois você não poderá recuperá-lo mais tarde.

6. Copie o valor do segredo do cliente e a data de expiração.
7. No Studio, edite a conexão correspondente e substitua o conteúdo nos campos **Segredo do aplicativo** e **Data de expiração do segredo** pelos valores que você copiou.

ALTERAR A DATA DE EXPIRAÇÃO DO SEGREDO

Você pode usar o Studio para adicionar ou modificar a data de expiração do segredo do aplicativo em uso.

1. No assistente **Adicionar Conexão e Recursos**, clique com o botão direito do mouse em uma conexão e clique em **Editar Conexão**.
2. Na página **Propriedades da Conexão**, clique em **Data de expiração do segredo** para adicionar ou modificar a data de expiração do segredo do aplicativo em uso.



Criar uma conexão de host usando a Identidade Gerenciada do Azure

Você pode criar uma conexão de host com o Microsoft Azure Resource Manager usando a Identidade Gerenciada do Azure. As identidades gerenciadas do Azure oferecem uma maneira segura e escalável de acessar os serviços do Azure sem a necessidade de gerenciar credenciais. Essa abordagem elimina os riscos associados ao armazenamento, rotação e gerenciamento de segredos.

O **Modo de Autenticação** tem três opções:

- AppClientSecret
- SystemAssignedManagedIdentity
- UserAssignedManagedIdentity

Antes de começar

A seguir estão as etapas que você deve seguir antes de criar a conexão de host usando a Identidade Gerenciada do Azure:

1. Instale um Citrix Cloud Connector™ em uma VM do Azure.
2. Habilite a Identidade Gerenciada do Azure nessa VM do Cloud Connector.
    - Para a identidade gerenciada atribuída pelo usuário:
        a. No portal do Azure, crie uma identidade gerenciada atribuída pelo usuário. Para obter informações, consulte Criar e atribuir uma Identidade Gerenciada Atribuída pelo Usuário.
        b. Atribua funções do Azure à identidade gerenciada. Consulte Permissões do Azure necessárias.
        c. Crie uma VM do Azure como um Cloud Connector e adicione a identidade atribuída pelo usuário a ela.
    - Para a identidade gerenciada atribuída ao sistema:
        a. Abra o portal do Azure e vá para sua VM.
        b. Selecione o painel Identidade nas configurações da VM.
        c. Na guia **Atribuído ao sistema**, defina o status como **Ativado**.
        d. Clique em **Salvar**.
        e. Conceda Permissões do Azure necessárias.

> **Nota:**
>
> Se você habilitar a identidade gerenciada atribuída ao sistema em uma VM do Cloud Connector e usá-la para criar uma conexão de host, ainda poderá criar conexões de host com a identidade gerenciada atribuída ao sistema mesmo depois de desativá-la na VM do Cloud Connector. A criação de conexões de host pode ser bem-sucedida mesmo 24 horas após a identidade ter sido desativada. Isso acontece porque os tokens de identidade gerenciada são armazenados em cache pela infraestrutura subjacente do Azure. Para obter mais informações, consulte Os tokens de identidades gerenciadas são armazenados em cache?.

Crie a conexão de host com a Identidade Gerenciada do Azure usando o Studio

No assistente **Adicionar Conexão e Recursos**:

1. Na página **Conexão**:

a. Selecione **Criar uma nova conexão**, o tipo de conexão do Microsoft Azure e seu ambiente Azure.

b. Selecione quais ferramentas usar para criar as máquinas virtuais e, em seguida, selecione Avançar.

2. Na página **Detalhes da Conexão**, selecione o **Modo de autenticação**.

- Para a **Identidade gerenciada atribuída pelo usuário**, insira as seguintes configurações. Depois de inserir os detalhes, selecione **Avançar** para prosseguir para as páginas seguintes. Você não pode avançar além desta página até fornecer detalhes válidos.

  - **ID da Assinatura**: Insira seu ID da assinatura do Azure. Para obter seu ID da assinatura, faça login no portal do Azure e navegar para **Assinaturas > Visão geral**.
  - **ID do Active Directory** (ID do locatário): Insira o ID do Diretório (locatário) do aplicativo que você registrou no Microsoft Entra ID.
  - **ID do Cliente**: Insira o ID do Cliente da Identidade Gerenciada que você criou no portal do Azure.
  - **URL de Autenticação**: Este campo é preenchido automaticamente e não é editável.
  - **URL de Gerenciamento**: Este campo é preenchido automaticamente e não é editável.
  - **Sufixo de armazenamento**: Este campo é preenchido automaticamente e não é editável.

- Para a **Identidade gerenciada atribuída ao sistema**, insira as seguintes configurações. Depois de inserir os detalhes, selecione **Avançar** para prosseguir para as páginas seguintes. Você não pode avançar além desta página até fornecer detalhes válidos.

  - **ID da Assinatura**: Insira seu ID da assinatura do Azure. Para obter seu ID da assinatura, faça login no portal do Azure e navegar para **Assinaturas > Visão geral**.
  - **ID do Active Directory** (ID do locatário): Insira o ID do Diretório (locatário) do aplicativo que você registrou no Microsoft Entra ID.
  - **URL de Autenticação**: Este campo é preenchido automaticamente e não é editável.
  - **URL de Gerenciamento**: Este campo é preenchido automaticamente e não é editável.
  - **Sufixo de armazenamento**: Este campo é preenchido automaticamente e não é editável.

Criar a conexão de host com o Azure Managed Identity usando PowerShell

Você pode criar esta conexão de host usando uma nova CustomProperty `AuthenticationMode`. O `AuthenticationMode` tem três opções: `AppClientSecret`, `SystemAssignedManagedIdentity` e `UserAssignedManagedIdentity`. A seguir, a descrição das opções do modo de autenticação:

- `AppClientSecret`: Este é o valor padrão. Isso requer um ID de Aplicativo e um segredo.
- `UserAssignedManagedIdentity`: Isso requer que um ID de cliente seja fornecido através de um UserName.
- `SystemAssignedManagedIdentity`: Isso não requer nenhuma entrada. Mesmo que você forneça um ID de cliente, ele será ignorado.

> **Nota:**
>
> Ao usar o PowerShell, o parâmetro `ProxyHypervisorTrafficThroughConnector` deve ser verdadeiro para usar a identidade gerenciada.

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie conexões de host. Por exemplo:
    - Para a identidade gerenciada atribuída ao usuário:

```
$UserName = "should be the Client ID of the user-assigned managed
identity"

$Password = "It can be any string.Not used"



$CustomProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">' `

+ '<Property xsi:type="StringProperty" Name="SubscriptionId"
Value="' + $SubscriptionId + '" />'`

+ '<Property xsi:type="StringProperty" Name="ManagementEndpoint"
```

```
Value="https://management.azure.com/" />'`

+ '<Property xsi:type="StringProperty"
Name="AuthenticationAuthority" Value="https://
login.microsoftonline.com/" />'`

+ '<Property xsi:type="StringProperty" Name="StorageSuffix"
Value="core.windows.net" />'`

+ '<Property xsi:type="StringProperty" Name="TenantId" Value="' +
$TenantId + '" />'`

+ '<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True" />'`

+ '<Property xsi:type="StringProperty" Name="AuthenticationMode"
Value="UserAssignedManagedIdentity" />'`

+ '</CustomProperties>'



New-Item -ConnectionType "Custom" `

-CustomProperties $CustomProperties `

-HypervisorAddress @($HypervisorAddress) `

-Path @("XDHyp:\Connections\$($ConnectionName)") `

-Metadata $Metadata `

-Persist `

-PluginId "AzureRmFactory" `

-Scope @() `

-Password $Password `

-UserName $UserName `
```

```
-ZoneUid $zoneUid
```

- Para a identidade gerenciada atribuída ao sistema:

```
$UserName = "It can be any string. Not used"

$Password = "It can be any string. Not used"

$CustomProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">' `

+ '<Property xsi:type="StringProperty" Name="SubscriptionId"
Value="' + $SubscriptionId + '" />'`

+ '<Property xsi:type="StringProperty" Name="ManagementEndpoint"
Value="https://management.azure.com/" />'`

+ '<Property xsi:type="StringProperty"
Name="AuthenticationAuthority" Value="https://
login.microsoftonline.com/" />'`

+ '<Property xsi:type="StringProperty" Name="StorageSuffix"
Value="core.windows.net" />'`

+ '<Property xsi:type="StringProperty" Name="TenantId" Value="' +
$TenantId + '" />'`

+ '<Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="True" />'`

+ '<Property xsi:type="StringProperty" Name="AuthenticationMode"
Value="SystemAssignedManagedIdentity" />'`

+ '</CustomProperties>'



New-Item -ConnectionType "Custom" `

-CustomProperties $CustomProperties `
```

```
-HypervisorAddress @($HypervisorAddress) `

-Path @("XDHyp:\Connections\$($ConnectionName)") `

-Metadata $Metadata `

-Persist `

-PluginId "AzureRmFactory" `

-Scope @() `

-Password $Password `

-UserName $UserName `

-ZoneUid $zoneUid
```

Gerenciar o Azure Managed Identity de uma conexão de hospedagem existente

Usar o Studio

Após criar uma conexão de hospedagem, você pode optar por atualizar a conexão de hospedagem existente para ter:

- Identidade gerenciada atribuída pelo sistema
- Identidade gerenciada atribuída pelo usuário
- Uma nova identidade gerenciada atribuída pelo usuário

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e, em seguida, selecione **Editar Conexão** na barra de ações.
3. Na página **Propriedades da Conexão** que aparece, clique em **Editar modo de autenticação**. Agora você pode optar por atualizar o modo de autenticação.
    - Clique em **Identidade gerenciada atribuída pelo usuário** para usar a identidade gerenciada atribuída pelo usuário para essa conexão de hospedagem. Siga o ID do Cliente a ser preenchido.
    - Clique em **Identidade gerenciada atribuída pelo sistema** para usar a identidade gerenciada atribuída pelo sistema para essa conexão de hospedagem.

Usar o PowerShell

Você também pode atualizar uma conexão de host existente usando o PowerShell para usar uma identidade atribuída pelo sistema ou uma identidade gerenciada atribuída pelo usuário. Por exemplo, execute os seguintes comandos do PowerShell:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Execute os seguintes comandos:

```
$connName = "ConnectionName"

$conn = get-item XDHyp:\Connections\$connName

$conn.CustomProperties
```

4. Mude `ProxyHypervisorTrafficThroughConnector` para `True` e adicione a propriedade personalizada para `AuthenticationMode` definida como `SystemAssignedManagedIdentity` ou `UserAssignedManagedIdentity`. Por exemplo:

```
$customProps = '<CustomProperties xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation"><Property xsi:type="StringProperty"
Name="SubscriptionId" Value="subscriptionId" /><Property
xsi:type="StringProperty" Name="ManagementEndpoint" Value="https://
management.azure.com/" /><Property xsi:type="StringProperty"
Name="AuthenticationAuthority" Value="https://
login.microsoftonline.com/" /><Property xsi:type="StringProperty"
Name="StorageSuffix" Value="core.windows.net" /><Property
xsi:type="StringProperty" Name="TenantId" Value="tenantId" /><Property
xsi:type="StringProperty" Name="AzureAdDeviceManagement"
Value="false" /><Property xsi:type="StringProperty"
Name="ProxyHypervisorTrafficThroughConnector" Value="true" /><Property
xsi:type="StringProperty" Name="AuthenticationMode"
Value="SystemAssignedManagedIdentity" /></CustomProperties>'
```

5. Execute `$cred = Get-Credential`. Insira qualquer coisa aqui.
6. Execute `Set-Item -PSPath XDHyp:\Connections\$connName -CustomProperties $CustomProperties -username $cred.username -Securepassword $cred.password`.

Zonas Estendidas do Azure

As Zonas Estendidas do Azure são extensões de pequena pegada de regiões existentes do Azure, permitindo que as organizações executem cargas de trabalho mais perto de seus usuários para melhorar o desempenho e a conformidade. O MCS no Azure agora oferece suporte ao provisionamento e gerenciamento de energia para VMs em Zonas Estendidas.

Para saber mais sobre as Zonas Estendidas do Azure, consulte a documentação da Microsoft: documentação das Zonas Estendidas do Azure.

Casos de uso

Este recurso é aplicável para catálogos persistentes e não persistentes:

- VMs somente gerenciadas por energia: você pode importar suas VMs de zona estendida existentes para um catálogo somente gerenciado por energia e gerenciá-las com o Citrix MCS.
- VMs provisionadas pelo MCS: você pode provisionar novas VMs em uma Zona Estendida e gerenciá-las com o MCS. Este recurso também inclui suporte para fluxos de trabalho de gerenciamento de imagens.

Limitações

Atualmente, existem várias limitações para o uso das Zonas Estendidas do Azure. Muitas dessas limitações são devido às restrições atuais do Azure:

- Hosts dedicados não são suportados.
- Reservas de capacidade não são suportadas.
- Grupos de posicionamento por proximidade não são suportados.
- VMs Spot não são suportadas.
- Zonas de Disponibilidade não são suportadas em Zonas Estendidas.
- Apenas os tipos de armazenamento **StandardSSD_LRS** e **Premium_LRS** são suportados.
- Atualmente, você não pode usar o recurso **UseSharedImageGallery** para salvar uma imagem mestre em uma Galeria de Computação do Azure (ou Galeria de Imagens Compartilhadas) em uma Zona Estendida. Como um subproduto, os discos de SO efêmeros também não são suportados.
- Se você estiver usando uma versão de imagem da Galeria de Computação do Azure como sua imagem mestre, certifique-se de que a replicação foi totalmente concluída na Zona Estendida antes de tentar usá-la. Tentar usar a versão da imagem antes que a replicação seja concluída pode resultar em falha na implantação.

Pré-requisitos

Antes de usar as Zonas Estendidas, certifique-se de ter concluído as seguintes etapas de pré-requisito:

1. Registrar no Azure:
    a. As Zonas Estendidas não são habilitadas por padrão.
    b. Registre o provedor de recursos `Microsoft.EdgeZones` em sua assinatura do Azure: Registre sua assinatura para o provedor de recursos Microsoft.EdgeZones.
    c. Registre cada Zona Estendida necessária separadamente (ex: LosAngeles, Perth): Registrar para uma Zona Estendida do Azure.
2. Preparar recursos Citrix:
    a. Crie uma rede virtual em sua Zona Estendida.
    b. Crie imagens mestre e instantâneos conforme necessário.

Permissões necessárias

Para criar um catálogo em uma Zona Estendida, seu principal de serviço deve ter a seguinte permissão: `Microsoft.EdgeZones/extendedZones/read`.

Para obter mais informações sobre as permissões mínimas necessárias, consulte Permissões mínimas.

Etapas de configuração

1. Criar uma Unidade de Hospedagem em uma Zona Estendida

    As Zonas Estendidas, que usam o tipo `.extendedzone`, são listadas junto com as regiões no inventário do Citrix MCS. Para provisionar em uma zona estendida, você deve criar uma nova unidade de hospedagem vinculada a essa zona estendida.

    Exemplo: Para criar uma Unidade de Hospedagem na Zona Estendida de Los Angeles

```
$RootPath = "XDHyp:\Connections\MyConnectionName\Los
Angeles.extendedzone"



$NetworkPath = "XDHyp:\Connections\MyConnectionName\Los
Angeles.extendedzone\virtualprivatecloud.folder\MyResourceGroup.resourc
egroup\MyExtendedZoneNetwork.virtualprivatecloud\MyExtendedZoneSubnet.n
```

```
etwork"



$HostingUnitPath = "XDHyp:\HostingUnits\MyHostingUnitName"



New-Item -HypervisorConnectionName MyConnectionName -NetworkPath
@($NetworkPath) -Path @($HostingUnitPath) -RootPath $RootPath
-StoragePath @()
```

2. Criar um Catálogo MCS em uma Zona Estendida

   Após criar sua Unidade de Hospedagem, prossiga com a criação do catálogo usando o Studio ou o PowerShell. Certifique-se de que seu catálogo faça referência à Unidade de Hospedagem da Zona Estendida.

Solução de problemas

Se você encontrar problemas, verifique o seguinte:

1. Certifique-se de que sua assinatura esteja registrada para zonas estendidas.
   a. Confirme se sua assinatura está registrada com o provedor de recursos Microsoft.EdgeZones.
   b. Certifique-se de que cada Zona Estendida seja registrada individualmente.
2. Verifique se seu principal de serviço tem a nova permissão.
   a. Seu principal de serviço deve ter a permissão `Microsoft.EdgeZones/extendedZones/read`.

Itens de inventário em Zonas Estendidas podem ser mostrados como "Zona Estendida Desconhecida" se o registro ou as permissões estiverem faltando.

> **Nota:**
>
> Se você estiver criando um catálogo na região pai usando uma imagem mestre de uma Zona Estendida, o registro e as permissões para a Zona Estendida ainda serão necessários.

Usar um grupo de segurança de rede pré-criado

Crie um grupo de segurança de rede Deny-All para preparação de imagem em vez de solicitar que a Citrix crie e modifique o NSG. Edite as propriedades personalizadas da unidade de hospedagem usando um comando PowerShell `Set-Item` para incluir o parâmetro `NsgForPreparation` para fornecer o grupo de segurança de rede Deny-All.

Pré-requisitos

Configure as seguintes permissões necessárias para uma entidade de serviço:

- `Microsoft.Network/networkSecurityGroups/join/action`: Associar um grupo de segurança de rede a uma sub-rede ou interface de rede
- `Microsoft.Network/networkSecurityGroups/read`: Obtém o grupo de segurança de rede
- `Microsoft.Network/networkSecurityGroups/securityRules/read`: Obtém a regra

Adicionar o grupo de segurança de rede Deny-All pré-criado

Para adicionar o grupo de segurança de rede Deny-All pré-criado, defina as propriedades personalizadas da seguinte forma na unidade de hospedagem:

1. Abra uma janela do PowerShell usando o SDK do PowerShell Remoto.
2. Execute os seguintes comandos:

```
Add-PSSnapin citrix*.

cd XDHyp:\HostingUnits\

Dir
```

3. Selecione uma unidade de hospedagem para recuperar os detalhes:

```
Get-Item "XDHyp:\HostingUnits\<hostingunitname>"
```

4. Copie as CustomProperties para um bloco de notas e anexe a configuração da propriedade `<Property xsi:type="StringProperty` " Name= `"NsgForPreparation` " Value= `"{ResourceGroupName}/{NetworkSecurityGroupName}"/>`. Por exemplo:

```
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
```

```
Name=`"NsgForPreparation`" Value=`{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>
```

5. Na janela do PowerShell, atribua uma variável às propriedades personalizadas modificadas. Por exemplo:

```
$customProperty = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`"{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>"
```

6. Execute `$cred = Get-Credential`. Se solicitado, forneça as credenciais de conexão. As credenciais são ID do Aplicativo Azure e segredo.
7. Execute o seguinte comando.

```
Set-Item -PSPath XDHyp:\HostingUnits\<hostingunitname>
-CustomProperties $customProperty -username $cred.username
-Securepassword $cred.password
```

Importante:

Se você receber uma mensagem informando que SubscriptionId está faltando, substitua todas as aspas duplas (“) por um acento grave seguido de aspas duplas (`”) na propriedade personalizada.

8. Execute `dir` para verificar as configurações `CustomProperties` atualizadas.

Nota:

Leva mais de um minuto para que as atualizações sejam refletidas.

Recuperar detalhes do grupo de segurança de rede

Para recuperar os detalhes do grupo de segurança de rede, primeiro recupere os grupos de recursos que contêm o grupo de segurança de rede e, em seguida, recupere o grupo de segurança de rede com base no nome do grupo de recursos.

1. Recupere os grupos de recursos que contêm o grupo de segurança de rede. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes":
["networksecuritygroup"]}'
```

2. Recupere o grupo de segurança de rede com base no nome do grupo de recursos. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType securitygroup -MaxRecords
5 -AdditionalDataFilter '{"location": ["eastus", "westus"],
"resourcegroup":["resourcegroupname"]}'
```

Filtrar grupos de recursos vazios

Use o comando PowerShell `Get-HypInventoryItem` para filtrar grupos de recursos vazios ao selecionar uma imagem mestre, perfil de máquina ou imagem preparada durante a criação do catálogo de máquinas.

Exemplos:

- Recuperar o número máximo de registros em uma página:

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- Recuperar o número máximo de registros em uma página e filtrar para encontrar contêineres de recursos que tenham recursos específicos.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- Recuperar com salto para indicar diretamente a página e filtrar para encontrar contêineres de recursos que tenham recursos específicos.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -skip 20 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- Usar um token para recuperar a próxima página e filtrar para encontrar contêineres de recursos que tenham recursos específicos.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
-ContinuationToken
'ew0KICAiJGlkIjogIjEiLA0KICAiTWF4Um93cyI6IDUsDQogICJSb3dzVG9Ta2lwIjogMj
UsDQogICJLdXN0b0NsdXN0ZXJVcmwiOiAiaHR0cHM6Ly9hcmctbmV1LTEzLXNmLmFyZy5jb
3JlLndpbmRvd3MubmV0Ig0KfQ=='
```

- Recuperar todos os grupos de recursos com a tag interna do Citrix e limitar o número máximo de registros com `MaxRecords`.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- Filtrar por perfil de máquina (imagem mestre) com a tag interna do Citrix e limitar o número máximo de registros com `MaxRecords`.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- Filtrar por imagem preparada com a tag interna do Citrix e limitar o número máximo de registros com `MaxRecords`.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
```

```
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion"]}'
```

- Filtrar por perfil de máquina (imagem preparada) com a tag interna do Citrix e limitar o número máximo de registros com `MaxRecords`.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- Filtrar por imagem com a tag interna do Citrix e limitar o número máximo de registros com `MaxRecords` e localização.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"], "location": ["eastus",
"westus"]}'
```

- Recuperar todos os grupos de recursos sem considerar as tags `CitrixResource`.

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
50 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"]}' -Force $true
```

Permissões do Azure necessárias

Esta seção detalha as permissões mínimas e as permissões gerais necessárias para o Azure.

Permissões mínimas

As permissões mínimas oferecem melhor controle de segurança. No entanto, novos recursos que exigem permissões adicionais falham se apenas as permissões mínimas forem concedidas. Esta seção lista as permissões mínimas por ação.

CRIANDO UMA CONEXÃO DE HOST

Adicione uma conexão de host usando as informações obtidas do Azure.

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",

"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/tenants/read",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read",

"Microsoft.EdgeZones/extendedZones/read"
```

GERENCIAMENTO DE ENERGIA DE VMS

Ligue ou desligue as instâncias da máquina.

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

CRIANDO, ATUALIZANDO OU EXCLUINDO VMS

Crie um catálogo de máquinas, adicione, exclua, atualize máquinas e exclua o catálogo de máquinas.

A seguir está a lista de permissões mínimas necessárias quando as imagens mestre são discos gerenciados ou instantâneos que estão na mesma região da conexão de hospedagem.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",
```

```
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Features/providers/features/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read",

"Microsoft.Compute/capacityReservationGroups/deploy/action"
```

Você precisa das seguintes permissões extras com base nas permissões mínimas para os seguintes recursos:

- Se a imagem mestre for um VHD em uma conta de armazenamento na mesma região da conexão de hospedagem:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",
```

- Se a imagem mestre for uma ImageVersion da Azure Compute Gallery (anteriormente Shared Image Gallery):

```
"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",
```

- Se a imagem mestre for um disco gerenciado, instantâneo ou VHD estiver em uma região diferente da região da conexão de hospedagem:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

- Se você usar o grupo de recursos gerenciado pela Citrix:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- Se você colocar a imagem mestre na Azure Compute Gallery (anteriormente Shared Image Gallery) em um locatário ou assinatura compartilhada:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Resources/subscriptions/read",
```

- Se você usar o suporte a host dedicado do Azure:

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- Se você usar a Criptografia do Lado do Servidor (SSE) com Chaves Gerenciadas pelo Cliente (CMK):

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- Se você implantar VMs usando modelos ARM (perfil de máquina):

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",

"Microsoft.Insights/DataCollectionRuleAssociations/Read",

"Microsoft.Insights/dataCollectionRules/read",
```

- Se você usar a especificação de modelo do Azure como um perfil de máquina:

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

CRIANDO, ATUALIZANDO E EXCLUINDO MÁQUINAS COM DISCO NÃO GERENCIADO

A seguir está a lista de permissões mínimas necessárias quando a imagem mestre é VHD e o grupo de recursos é fornecido pelo administrador:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

```
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read"
```

GERENCIAMENTO DE CUSTOS

A seguir está a permissão mínima necessária para recuperar o preço da VM:

```
"Microsoft.Consumption/pricesheets/read"
```

A seguir está a permissão mínima necessária para recuperar o custo da VM:

```
"Microsoft.CostManagement/query/read"
```

Nota:

Para visualizar a guia **Cost Insights** de um catálogo de máquinas do Azure, você deve ter a permissão **Gerenciamento de Custos > Gerenciar > Ler custo** (padrão para Administradores de Nuvem). Para obter informações sobre a guia **Cost Insights**, consulte Exibir detalhes do catálogo.

Permissões gerais

A função de Colaborador tem acesso total para gerenciar todos os recursos. Este conjunto de permissões não o impede de obter novos recursos.

O seguinte conjunto de permissões oferece a melhor compatibilidade daqui para frente, embora inclua mais permissões do que o necessário com o conjunto de recursos atual:

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/images/versions/write",
```

```
"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/write",

"Microsoft.Compute/hostGroups/hosts/read",

"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",
```

```
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
```

```
"Microsoft.Resources/subscriptions/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tenants/read",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
"Microsoft.Compute/capacityReservationGroups/capacityReservations/read",
"Microsoft.Consumption/pricesheets/read",
"Microsoft.Network/networkSecurityGroups/join/action",
```

```
"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read",

"Microsoft.Compute/capacityReservationGroups/deploy/action",

"Microsoft.EdgeZones/extendedZones/read"
```

Configurar as permissões necessárias para a conexão de host do Azure

Você pode configurar facilmente todas as permissões mínimas necessárias para uma entidade de serviço ou conta de usuário no Azure, vinculada a uma conexão de host, para executar todas as operações do MCS usando um modelo ARM. Este modelo ARM automatiza o seguinte:

- Criação de uma Função do Azure com as permissões mínimas necessárias para as operações.
- Atribuição desta função a um Azure Service Principal existente no nível da assinatura.

Você pode implantar este modelo ARM usando o Portal do Azure ou comandos do PowerShell. Para obter mais informações, consulte Modelo ARM para Operações do Citrix Virtual Apps and Desktops.

Validar permissões na conexão do host

Você pode validar as permissões em uma conexão de host para realizar tarefas relacionadas à criação e gerenciamento de catálogos de máquinas MCS. Essa implementação ajuda você a descobrir as permissões ausentes necessárias para diferentes cenários, como criar, excluir e atualizar VMs, gerenciamento de energia de VMs, com antecedência para que você possa evitar ser bloqueado em momentos críticos.

Você pode validar as permissões em uma conexão de host usando o comando PowerShell `Test-HypHypervisorConnection`. O resultado do comando é capturado como uma lista onde cada item da lista é dividido em três seções.

- Categoria: A ação ou tarefa que um usuário pode fazer para criar e gerenciar um catálogo de máquinas MCS.
- Ação Corretiva: A etapa que um administrador deve realizar para resolver uma discrepância de permissões ausentes dos usuários.
- Permissão ausente: A lista de permissões ausentes para uma categoria.

Para validar as permissões, faça o seguinte:

1. Crie uma conexão de host com o Azure.
2. Abra uma janela do PowerShell a partir do host do Delivery Controller™.
3. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
4. Execute o seguinte comando para verificar se você tem as permissões necessárias para testar uma conexão.

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AzureCon"
   ```

   Permissão de nível de função necessária para o SPN:

   - Microsoft.Authorization/roleDefinitions/read (no nível da assinatura ou no nível do grupo de recursos, se o grupo de recursos for fornecido)
   - Microsoft.Authorization/roleAssignments/read (no nível da assinatura ou no nível do grupo de recursos, se o grupo de recursos for fornecido)

   Permissões de nível de API necessárias para o SPN:

   Microsoft.Graph:

   - Application.Read.All
   - Directory.Read.All
   - ServicePrincipalEndpoint.Read.All

5. Depois de adicionar as permissões ausentes necessárias para pesquisar suas permissões, execute o seguinte comando para verificar se você tem permissões nas várias categorias.

   Exemplo:

   Para testar uma conexão no nível da assinatura com um nível mais alto de autorização necessário:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\ AzureCon
   -SecurePassword $password -UserName 922e65d5-38ae-4cf5-xxxx-xxxxxxxxx
   ```

   Exemplo:

   Para testar uma conexão no nível do grupo de recursos sem um alto nível de autorização:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
-CustomProperties $customProperties | Format-List
```

Nota:

O parâmetro `CustomProperties` é usado para fornecer o nível do grupo de recursos porque o grupo de recursos é uma informação específica da conexão.

Exemplo:

Para testar uma conexão com o nível mais alto de autorização no nível do grupo de recursos:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
-SecurePassword $password -UserName
922e65d5-38ae-4cf5-832b-54122196b7dd -CustomProperties
$customProperties
```

Para obter informações sobre permissões, consulte Permissões do Azure necessárias.

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas do Azure, consulte Criar um catálogo do Microsoft Azure.

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização do Microsoft Azure Resource Manager

Conexão com o Microsoft SCVMM

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos do Microsoft System Center Virtual Machine Manager (VMM).

Nota:

> Antes de criar uma conexão com o VMM, você precisa primeiro concluir a configuração do seu VMM como um local de recurso. Consulte Ambientes de virtualização do Microsoft System Center Virtual Machine Manager.

Criar uma conexão

Se você usou o MCS para provisionar VMs, faça o seguinte no assistente de criação de conexão:

- Insira o endereço como um nome de domínio totalmente qualificado do servidor host.
- Insira as credenciais para a conta de administrador que você configurou anteriormente. Esta conta deve ter permissão para criar novas VMs.
- Na caixa de diálogo Detalhes do Host, selecione o cluster ou host autônomo a ser usado ao criar VMs.

> **Importante**
>
> Procure um cluster ou host autônomo mesmo se você estiver usando uma implantação de host Hyper-V único.

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para criar catálogos de máquinas com MCS em compartilhamento de arquivos SMB 3, consulte Criar um catálogo do Microsoft System Center Virtual Machine Manager.

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização do Microsoft System Center Virtual Machine Manager.

Conexão com Nutanix

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos do Nutanix.

> **Nota:**

> Antes de criar uma conexão com o Nutanix, você precisa primeiro concluir a configuração da sua conta Nutanix como um local de recurso. Consulte Ambientes de virtualização Nutanix.

Conexão de host Nutanix AHV Prism Central

Consulte os Pré-requisitos antes de criar a conexão de host Nutanix AHV Prism Central.

Você pode criar uma conexão usando um dos seguintes:

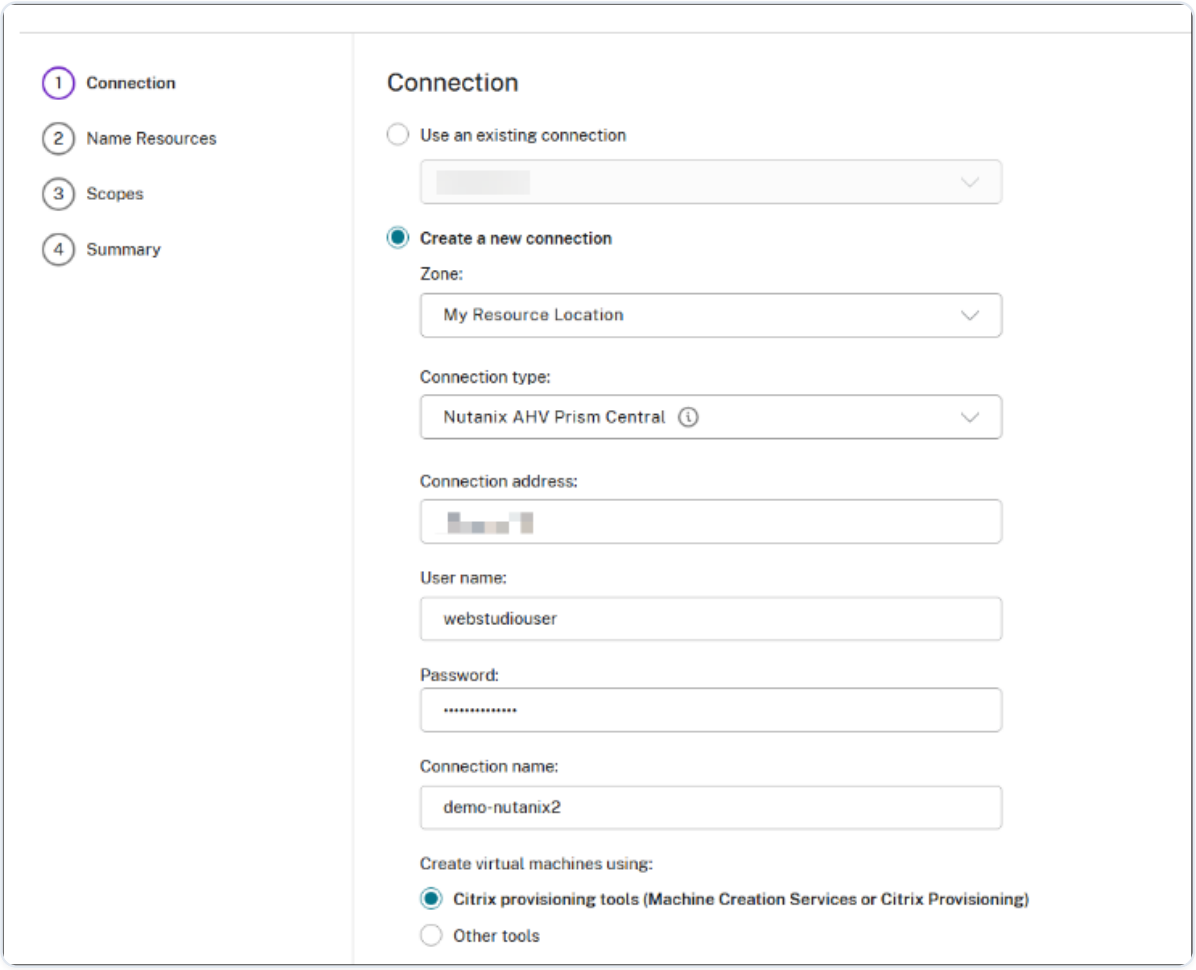
- Studio
- Comandos PowerShell

Limitação

- A conexão de host Nutanix AHV Prism Central não oferece suporte a nomes de objetos duplicados para itens como modelos e redes. A seleção de tais itens para a criação de catálogo pode levar a um comportamento inesperado.

Criar uma conexão usando o Studio

1. Faça login no Citrix Cloud.
2. No bloco DaaS, clique em **Gerenciar**.
3. Selecione **Hospedagem** no painel esquerdo.
4. Clique em **Adicionar Conexões e Recursos** na barra de ações.
5. Na página **Conexão**:
    a. Selecione **Criar uma nova conexão**.
    b. Selecione **Nutanix AHV Prism Central** como o tipo de conexão.
    c. Insira o endereço IP do seu Nutanix AHV Prism Central como o endereço de conexão.
    d. Insira suas credenciais administrativas e um nome de conexão amigável.
    e. Selecione **Ferramentas de provisionamento Citrix (Machine Creation Services™ ou Citrix Provisioning)**.
    f. Clique em **Avançar**.

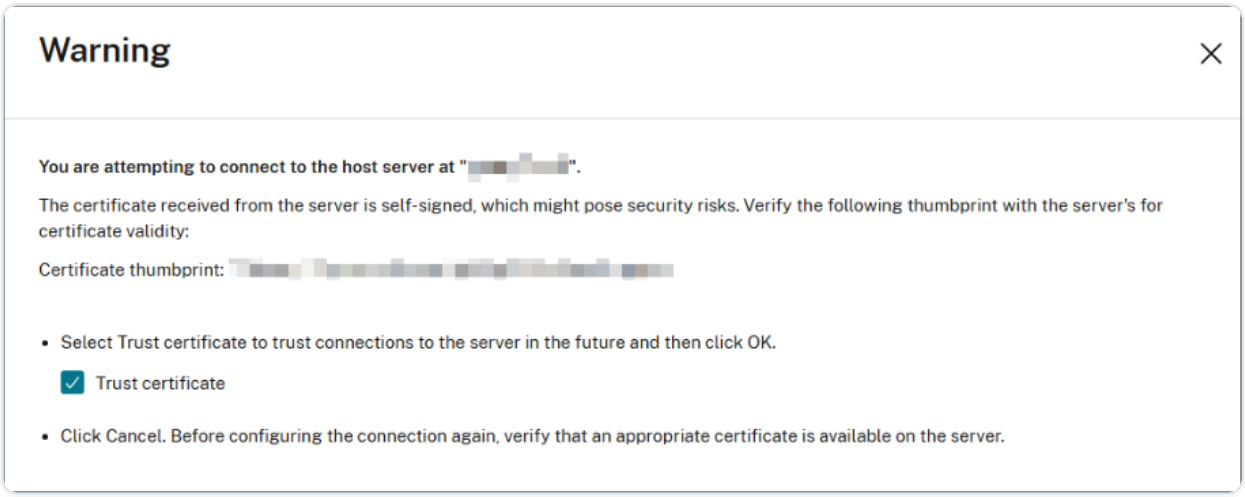


Nota:

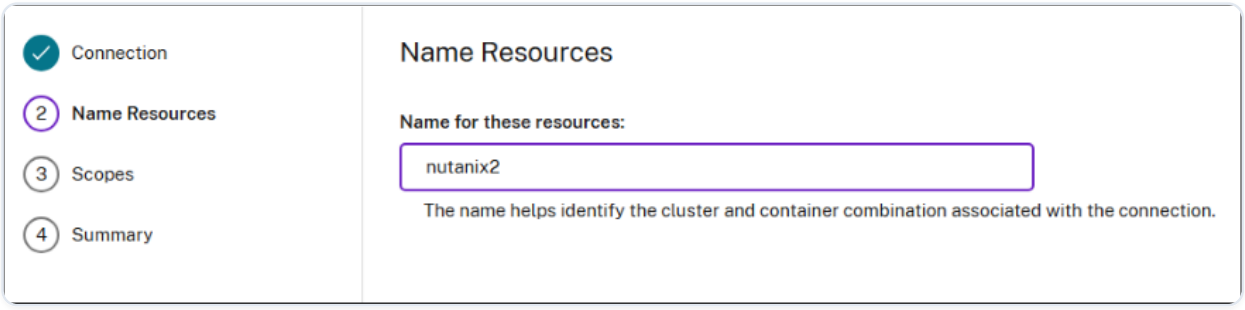
Ao criar a conexão do host, a seleção de rede ou cluster não é necessária. Apenas um nome de unidade de hospedagem é necessário. Selecione a rede e o cluster ao criar o catálogo de máquinas.

6. Depois de clicar em **Avançar**, o Citrix DaaS™ recebe um certificado privado assinado por CA e você verá uma página de **Aviso**. Para obter informações, consulte Conexões seguras com o Nutanix Prism Central.

   Compare o thumbprint recebido com o do servidor para a validade do certificado. Se for válido, selecione **Confiar no certificado** e clique em **OK** para prosseguir com a criação da conexão. O Citrix DaaS então confia no certificado e armazena o thumbprint para validação futura.



7. Na página **Nomear Recursos**, adicione um nome exclusivo para os recursos. Clique em **Avançar**.



8. Na página **Escopos**, selecione um ou mais escopos para este host.
9. Na página **Resumo**, verifique a configuração e clique em **Concluir**.

> **Observação:**
>
> A conexão Nutanix AHV Prism Central pode coexistir com outros tipos de conexões Nutanix.

Conexões seguras ao Nutanix Prism Central

O recurso de impressão digital SSL do Nutanix simplifica a confiança do certificado ao estabelecer uma conexão de host com um hipervisor Nutanix Prism Central. Este recurso permite o armazenamento da impressão digital de um certificado não confiável no banco de dados do site, garantindo que o Citrix DaaS reconheça consistentemente o hipervisor como confiável.

Ao criar uma conexão de host Nutanix, uma página de **Aviso** é exibida, apresentando o certificado da máquina à qual você está se conectando e permitindo que você decida se deseja confiar nele.

Criar uma conexão usando PowerShell

1. Abra a janela do PowerShell.

2. Execute `asnp citrix*`.
3. Defina os seguintes parâmetros:

```
$ConnectionName = “Name of the connection”

$UserName = “Username of the account on hypervisor”

$ZoneUid =  “UID of the zone where the hosting connection will be created”

$HypervisorAddress = “The IP address of the hypervisor”

$SSLThumbprint =  “The Nutanix PC SSL thumbprint can be set using PowerShell SDK”

$connectionPath = "XDHyp:\Connections\" + $ConnectionName

$SecureUserInput = Read-Host "Enter the password for the user $($UserName)" -AsSecureString

$EncryptedUserInput = $SecureUserInput | ConvertFrom-SecureString

$SecurePass = ConvertTo-SecureString -String $EncryptedUserInput
```

4. Crie um item para a nova conexão de hospedagem. Por exemplo:

```
$connection = New-Item -Path @($connectionPath) -ConnectionType "Custom" -HypervisorAddress ` @($HypervisorAddress) -Persist -PluginId "AcropolisHypervisorPCFactory" -Scope @() ` -SecurePassword $SecurePass -SSLThumbprint @($SSLThumbprint) -UserName $UserName -ZoneUid ` $ZoneUid
```

5. Crie uma conexão de hipervisor de broker. Por exemplo:

```
New-BrokerHypervisorConnection -HypHypervisorConnectionUid $connection.HypervisorConnectionUid
```

CRIAR UMA UNIDADE DE HOSPEDAGEM

Ao criar uma unidade de hospedagem usando o comando PowerShell, forneça os seguintes parâmetros obrigatórios:

- `$HostUnitName`: Nome da Unidade de Hospedagem a ser criada
- `ConnectionName`: Nome da conexão do hipervisor criada anteriormente

1. Abra a janela do PowerShell.
2. Execute `add-pssnapin citrix*`.
3. Execute comandos PowerShell para criar a unidade de hospedagem. Por exemplo:

```
$hostUnitPath = "XDHyp:\HostingUnits\" + $HostUnitName

New-Item -Path @($hostUnitPath) -RootPath $connectionPath
-HypervisorConnectionName $ConnectionName -CustomProperties ""
-NetworkPath @() -StoragePath @()
```

Nota:

Ao criar a conexão do host, a seleção de rede ou cluster não é necessária. Apenas um nome de unidade de hospedagem é necessário. Selecione a rede e o cluster ao criar o catálogo de máquinas.

Gerenciar conexões de host

Você pode gerenciar uma conexão de host existente usando:

- Studio
- PowerShell

GERENCIAR A CONEXÃO DO HOST USANDO O STUDIO

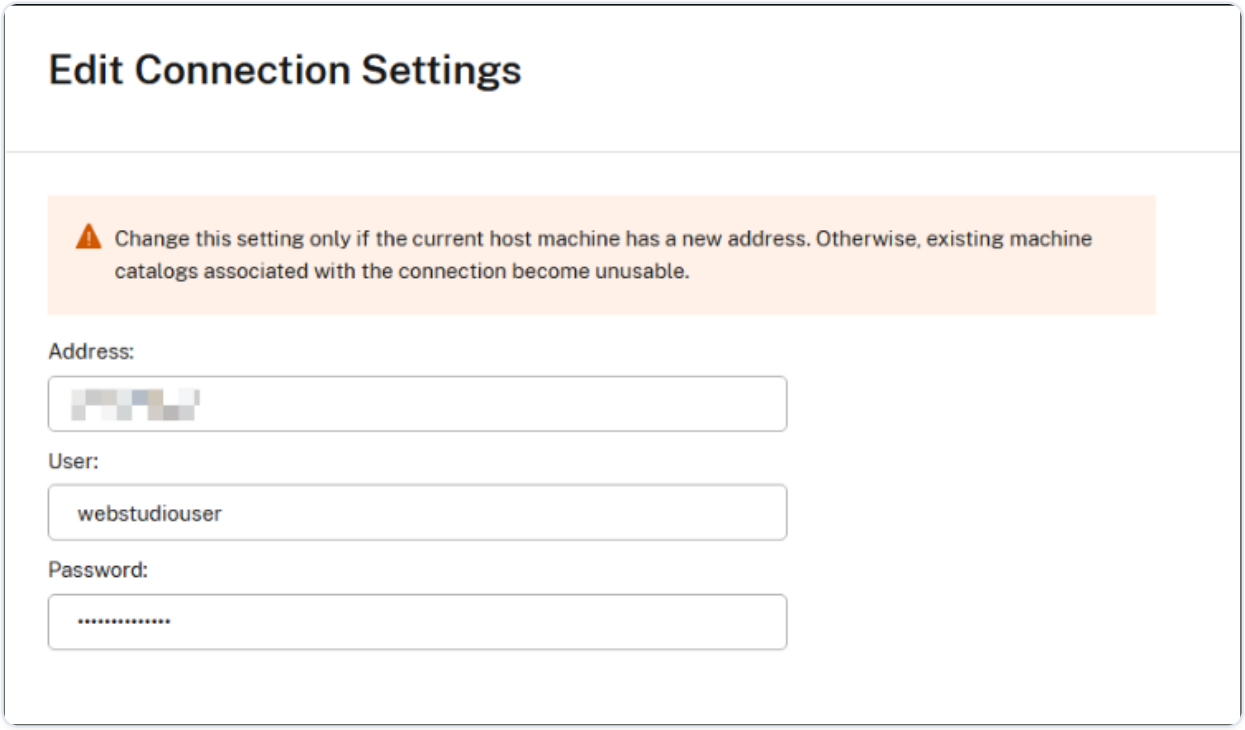
Após criar uma conexão de host, navegar até o nó **Hosting** no Studio e clique com o botão direito em uma conexão para fazer o seguinte:

- **Excluir Conexão**
- **Renomear Conexão**
- **Editar Conexão**
- **Ativar Modo de Manutenção**
- **Visualizar Máquinas**
- **Testar Conexão**

- **Testar confiança do certificado TLS**

EDITAR UMA CONEXÃO USANDO O STUDIO

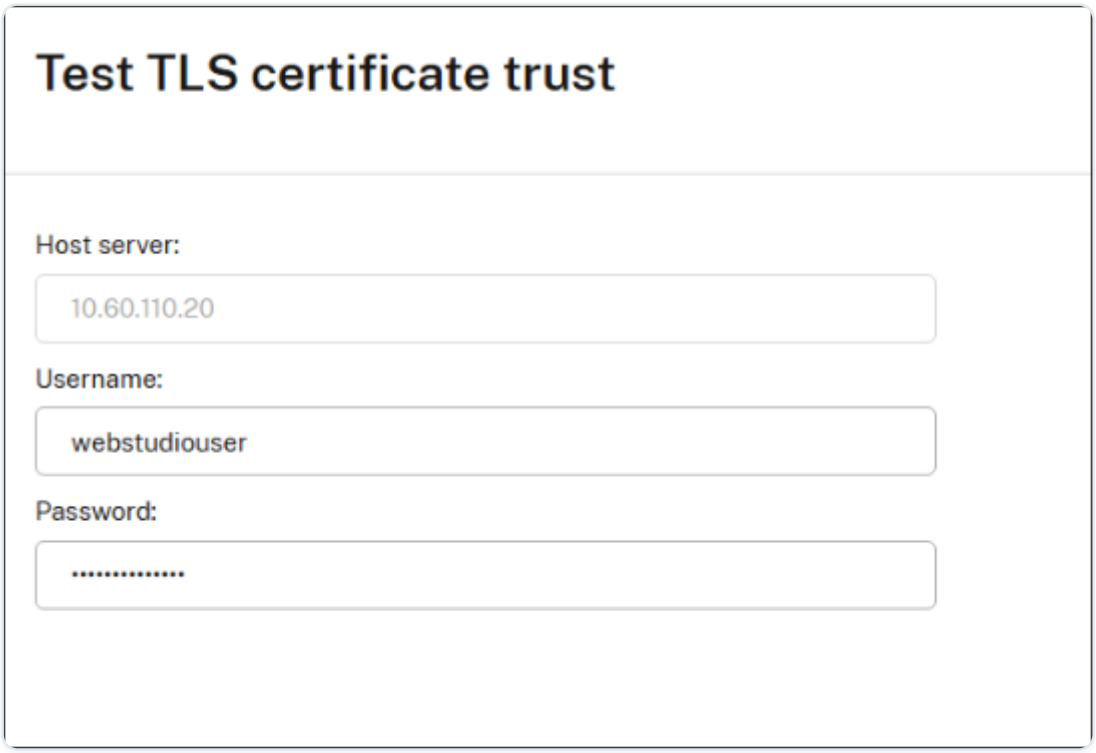
1. Clique com o botão direito em uma conexão e clique em **Editar Conexão**.
2. Na página **Propriedades da Conexão**, clique em **Editar configurações**.
3. Na página **Editar configurações de Conexão**, você pode alterar as informações do certificado e clicar em **Salvar**.



4. Selecione **Confiar no certificado** na página **Aviso** para confiar na nova impressão digital do certificado.

TESTAR CONFIANÇA DO CERTIFICADO TLS

1. Clique com o botão direito em uma conexão e clique em **Testar confiança do certificado TLS**.
2. Na página **Testar Confiança do Certificado TLS**, você pode alterar as informações do certificado e, em seguida, clicar em **Testar**.



Se o resultado do teste não for bem-sucedido, então altere as informações do certificado da conexão usando Editar uma conexão usando o Studio.

GERENCIAR A CONEXÃO DO HOST USANDO O POWERSHELL

Você pode usar comandos do PowerShell para:

- Alterar ou atualizar a credencial do usuário para uma conexão de host. Por exemplo:

```
$UserName = "Username of the account on hypervisor"

$SecureUserInput = Read-Host "Enter the password for the user $
($UserName)" -AsSecureString

$EncryptedUserInput = $SecureUserInput | ConvertFrom-SecureString

$SecurePass = ConvertTo-SecureString -String $EncryptedUserInput

Set-Item  -LiteralPath @("XDHyp:\Connections\<Host connection name>")
 -SecurePassword $SecurePass -UserName $UserName
```

- Redefinir SSLThumbprint. Por exemplo:

```
$SSLThumbprint =  "The Nutanix PC SSL thumbprint value"

Set-Item  -LiteralPath @("XDHyp:\Connections\<Host connection name>")
```

```
 -SecurePassword $SecurePass -UserName $UserName -SSLThumbprint
$SSLThumbprint
```

Permissões necessárias

As seguintes permissões são necessárias para a conta administrativa usada para uma conexão de host do Nutanix AHV Prism Central.

CRIANDO UMA CONEXÃO DE HOST

Cluster:

- Visualizar Cluster

GERENCIAMENTO DE ENERGIA DE VMS

AHV VM:

- Desligar Máquina Virtual ACPI
- Reiniciar Máquina Virtual ACPI
- Reiniciar Máquina Virtual Convidada
- Desligar Máquina Virtual Convidada
- Desligar Máquina Virtual
- Ligar Máquina Virtual
- Redefinir Máquina Virtual
- Visualizar Máquina Virtual Existente

Cluster:

- Visualizar Cluster

Sub-rede:

- Visualizar Sub-rede

PROVISIONAMENTO DE VMS

VM AHV:

- Reiniciar Máquina Virtual ACPI
- Desligar Máquina Virtual ACPI
- Associar Categorias de Máquina Virtual
- Criar Nova Máquina Virtual

- Criar Máquina Virtual
- Criar Disco de Máquina Virtual
- Criar NIC de Máquina Virtual
- Excluir Máquina Virtual Existente
- Excluir Máquina Virtual
- Excluir Disco de Máquina Virtual
- Excluir GPU de Máquina Virtual
- Excluir NIC de Máquina Virtual
- Desassociar Categorias de Máquina Virtual
- Ejetar CD ROM de Máquina Virtual
- Reiniciar Máquina Virtual (Convidado)
- Desligar Máquina Virtual (Convidado)
- Desligar Máquina Virtual
- Ligar Máquina Virtual
- Redefinir Máquina Virtual
- Snapshot de Máquina Virtual
- Atualizar Configuração Básica da Máquina Virtual
- Atualizar Disco da Máquina Virtual
- Atualizar Lista de Discos da Máquina Virtual
- Atualizar NIC da Máquina Virtual
- Visualizar Máquina Virtual Existente
- Visualizar Máquina Virtual
- Visualizar CD ROM da Máquina Virtual
- Visualizar Disco da Máquina Virtual
- Visualizar GPU da Máquina Virtual
- Visualizar NIC da Máquina Virtual

Ponto de Recuperação da VM AHV:

- Visualizar Ponto de Recuperação da VM AHV

Categoria:

- Visualizar Categoria

Cluster:

- Visualizar Cluster

Host:

- Visualizar Host

Imagem:

- Criar Imagem
- Excluir Imagem
- Atualizar Imagem
- Visualizar Imagem

Ponto de Recuperação:

- Criar Ponto de Recuperação
- Excluir Ponto de Recuperação
- Replicar Ponto de Recuperação
- Restaurar Ponto de Recuperação
- Visualizar Ponto de Recuperação
- Visualizar Ponto de Recuperação de Máquina Virtual

Contêiner de Armazenamento:

- Visualizar Contêiner de Armazenamento
- Visualizar Datastore do Contêiner de Armazenamento
- Visualizar Estatísticas do Contêiner de Armazenamento

Política de Armazenamento:

- Visualizar Política de Armazenamento

Sub-rede:

- Visualizar Sub-rede
- Visualizar Vnic da Sub-rede

Tarefa:

- Cancelar Tarefa
- Visualizar Tarefa

Ponto de Recuperação de VM:

- Excluir Ponto de Recuperação de VM
- Restaurar Ponto de Recuperação de VM
- Visualizar Ponto de Recuperação de VM

Modelos de VM:

- Visualizar Modelos de VM
- Visualizar Versões de Modelos de VM
- Implantar Modelos de VM

Grupo de Volumes:

- Anexar Grupo de Volumes à VM AHV
- Desanexar Grupo de Volumes da VM AHV
- Visualizar Grupo de Volumes
- Visualizar Detalhes do Grupo de Volumes

VPC:

- Visualizar VPC

Conexão de host Nutanix AHV, Nutanix AHV PC ou Nutanix AHV DRaaS

1. Faça login no Citrix Cloud.
2. No bloco DaaS, clique em **Gerenciar**.
3. Selecione **Hospedagem** no painel esquerdo.
4. Clique em **Adicionar Conexões e Recursos** na barra de ações.
5. Na página **Conexão**, os seguintes tipos de conexão estão disponíveis para seleção:

    - **Nutanix AHV**: especifique o endereço do cluster Prism Element (PE), as credenciais e um nome para a conexão. Na página **Rede**, selecione a(s) rede(s) e dê um nome para a unidade de hospedagem.

> **Nota:**
>
> Se você implantar máquinas usando o Nutanix AHV (Prism Element) como recurso, selecione o contêiner onde o disco da VM reside.

- **Nutanix AHV PC**: especifique o endereço do Prism Central (PC), as credenciais e um nome para a conexão. Na página **Rede**, selecione a rede, o cluster da lista e dê um nome para a unidade de hospedagem.

  > **Nota:**
  >
  > O tipo de conexão **Nutanix AHV PC** é usado apenas para criar conexão com o Nutanix Cloud Cluster (NC2) no Azure. Além disso, um catálogo de máquinas só pode ser hospedado em um único cluster em uma conexão NC2 no Azure. Este tipo de conexão requer um plug-in Nutanix instalado nos Cloud Connectors.

- **Nutanix AHV DRaaS**: especifique seu endereço e nome de usuário e, em seguida, importe as chaves públicas e privadas contidas em seus arquivos de credenciais do Nutanix DRaaS `.pem`. (As chaves públicas e privadas são geradas na nuvem Nutanix DRaaS pelos administradores do Nutanix DRaaS.)

  - Para importar a chave, localize seu arquivo de credenciais, abra-o com o Bloco de Notas (ou qualquer editor de texto) e, em seguida, copie o conteúdo. Depois disso, retorne à página **Conexão**, selecione **Importar chave**, cole o conteúdo e, em seguida, selecione **Salvar**. Não altere o conteúdo da credencial ou seu formato.

Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para informações específicas do Nutanix, consulte Criar um catálogo Nutanix.

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização Nutanix
- Soluções de nuvem e parceiros Nutanix

Conexão com a nuvem Nutanix e soluções de parceiros

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos da nuvem Nutanix e das soluções de parceiros.

Nutanix AHV Prism Central

O Citrix DaaS™ oferece suporte a Nutanix Cloud Clusters (NC2) nos seguintes hipervisores de nuvem para o plug-in Nutanix AHV Prism Central gerenciado pela Citrix.

- AWS
- Microsoft Azure

> **Nota:**
>
> - Antes de criar uma conexão com o NC2 na AWS e no Azure, prepare os recursos na plataforma de nuvem. Consulte Nutanix cloud and partner solutions.
> - Para as permissões para criar conexão de hospedagem, gerenciamento de energia de VMs e provisionamento de catálogos, consulte Required permissions.

Conectar-se ao NC2 no Azure e na AWS

A conexão a um Nutanix Cloud Cluster (NC2) no Azure ou na AWS requer acesso a uma instância do Prism Central implantada e credenciais com a função de Administrador do Prism.

Você pode criar uma conexão de host usando:

- Studio
- PowerShell

Para obter informações completas sobre a conexão, consulte Connection to Nutanix AHV Prism Central

Nutanix Prism Element

O Citrix DaaS suporta Nutanix Cloud Clusters (NC2) no seguinte hipervisor de nuvem para o plug-in Nutanix Prism Element.

- AWS

Conectar-se ao Nutanix Prism

Depois de criar um cluster Nutanix, conecte-se ao Nutanix Prism. Para se conectar ao Nutanix Prism:

1. Crie uma VM bastion na sub-rede 10.0.129.0/24.
2. Acesse a VM bastion via RDP, vá para a URL do **Prism Element** que você copiou na seção anterior.
3. Faça login usando as credenciais padrão: `admin:nutanix/4u`. Lembre-se de alterar a senha.

Crie uma VM no Cluster Nutanix

Após conectar-se ao **Nutanix Prism**, crie VMs no cluster Nutanix.

SE A VM PRECISAR DE ACESSO À INTERNET

1. Vá para o console da AWS.
2. Crie uma nova sub-rede 10.0.130.0/24 na mesma VPC que a criada pelo Nutanix CFS.
3. Adicione uma rota à tabela de rotas desta sub-rede para direcionar todo o tráfego não local para o gateway NAT acima.
4. Acesse a VM bastion via RDP, vá para a URL do **Prism Element** que você copiou na seção anterior e faça login.
5. Adicione uma nova rede. Vá para **Settings>Network Configuration>Create Subnet**. Use a mesma sub-rede 10.0.130.0/24 usada na AWS.
6. Crie todas as VMs (AD, CC, VDA e assim por diante) nessa nova sub-rede.

SE A VM NÃO PRECISAR DE ACESSO À INTERNET

1. Faça RDP na VM bastion, vá para a URL do **Prism Element** que você copiou na seção anterior e faça login.
2. Adicione uma nova rede. Vá para **Settings>Network Configuration>Create Subnet**. Use a sub-rede 10.0.129.0/24.
3. Crie todas as VMs (AD, CC, VDA e assim por diante) nessa sub-rede.

> **Dica:**

> Certifique-se de que as informações de hora e fuso horário nas VMs estejam configuradas corretamente. Isso é especialmente verdadeiro para o AD.

Criar conexão de host

1. No Studio, selecione **Hosting** no painel esquerdo.
2. Clique em **Adicionar Conexão e Recursos**.
3. Na tela **Conexão**, selecione **Criar uma nova Conexão** e, no **Endereço da conexão**, insira `https://xxx.xxx.xxx.xxx:9440`.
4. Siga a interface do usuário para concluir o assistente.

> **Nota:**
>
> Todas as VMs do conector devem ter o plug-in Nutanix instalado para que a opção Nutanix esteja disponível no Citrix Studio, mesmo que os plug-ins não sejam usados na zona Nutanix.

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para informações específicas do Nutanix, consulte Criar um catálogo Nutanix.

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização Nutanix
- Soluções de nuvem e parceiros Nutanix

Conexão com Red Hat OpenShift

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos do Red Hat OpenShift.

> **Nota:**
>
> Antes de criar uma conexão com o Red Hat OpenShift, você precisa primeiro concluir a configuração do seu Red Hat OpenShift. Consulte Ambientes de virtualização do Red Hat OpenShift.

Criar uma conexão

Você pode criar uma conexão com o cluster Red Hat OpenShift usando:

- Studio
- PowerShell

Criar uma conexão usando o Studio

1. navegar até **Hospedagem > Adicionar Conexão e Recursos**.
2. Na página **Conexão**, siga estas etapas para configurar a conexão:
    a. Selecione **Criar uma nova conexão**.
    b. Selecione **Red Hat OpenShift** como o tipo de conexão.
    c. No campo **Endereço da conexão**, insira o endereço IP, nome do host ou FQDN do servidor OpenShift.
    d. Insira seu token de conta de serviço e um nome de conexão amigável.
    e. Selecione uma zona no campo **Nome da zona**. As opções são todos os locais de recursos que você configurou.
    f. Selecione **Outras ferramentas** para criar máquinas virtuais.

    > **Nota:**
    >
    > A seleção de **Outras ferramentas** cria apenas a conexão de hospedagem sem uma unidade de hospedagem.

3. Clique em **Avançar**.
4. Se um certificado autoassinado for detectado, uma página de aviso aparecerá com a impressão digital do certificado. Para prosseguir:
    a. Compare a impressão digital com a do servidor para verificar a validade do certificado.
    b. Se for válido, selecione **Confiar no certificado** e clique em **OK** para concluir a configuração da conexão.

    O certificado é marcado como confiável e a impressão digital é salva para validação futura.
5. Na página **Escopos**, selecione um ou mais escopos para este host.
6. Na página **Resumo**, verifique a configuração e clique em **Concluir**.

Criar uma conexão usando comandos PowerShell

Ao criar uma conexão usando o comando PowerShell, forneça as seguintes informações:

- Nome da conexão de hospedagem
- Endereço da API do cluster
- Nome de usuário
- Senha (token da conta de serviço)
- SSLThumbprint: Esta é uma impressão digital de certificado CA e não a impressão digital do servidor API. O servidor fornece a impressão digital do certificado CA se você tentar criar uma conexão de hospedagem sem especificar a impressão digital.
- ZoneUid

1. Abra a janela do PowerShell.
2. Execute `add-pssnapin citrix*`.
3. Execute o seguinte comando para criar a conexão de hospedagem.

   Se você tentar criar uma conexão de hospedagem sem especificar a impressão digital, o servidor fornecerá a impressão digital do certificado CA. Por exemplo:

```
$newItemParameters = @{

ConnectionType= "Custom"

PluginId= "OpenShiftPluginFactory"

HypervisorAddress = "https://
api.myopenshiftclusteraddress.mydomain.local:6443"

Path= "XDHyp:\Connections\OpenShiftConnectionName"

Persist= $true

UserName= "__ServiceAccount__"

Password= "<service account token>"

ErrorVariable= "connectionError"

 }
```

```
& New-Item @newItemParameters




$newItemParameters["SSLThumbprint"] =
$connectionError[0].ErrorData.Thumbprint

$connection = & New-Item @newItemParameters

$brokerConnection = New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $connection.HypervisorConnectionUid
```

Criar uma unidade de hospedagem

Uma unidade de hospedagem representa um ambiente onde as VMs são criadas. Para criar a unidade de hospedagem, você precisa das seguintes entradas do OpenShift:

- Namespace
- StorageClasses
- Definição de Anexo de Rede

Uma unidade de hospedagem é vinculada a um namespace. Isso significa que uma unidade de hospedagem pode acessar apenas um namespace e gerencia as VMs sob esse namespace.

Você pode criar uma unidade de hospedagem usando:

- Studio
- PowerShell

Criar unidades de hospedagem usando o Studio

1. navegar para **Hosting > Add Connection and Resources**.
2. Na página **Connection**:
    - Para criar uma nova conexão de hospedagem juntamente com uma unidade de hospedagem, selecione **Create a new connection** e, em seguida, faça o seguinte:
        a. Selecione **Red Hat OpenShift** como o tipo de conexão.

b. No campo **Connection address**, insira o endereço IP, nome do host ou FQDN do servidor OpenShift.

c. Insira seu token de conta de serviço e um nome de conexão amigável.

d. Selecione uma zona no campo **Zone name**. As opções são todos os locais de recurso que você configurou.

e. Selecione **Citrix provisioning tools (Machine Creation Services™ or Citrix Provisioning) for creating virtual machines**.

f. Clique em **Next**.

g. Na página **Warning**, verifique a validade do certificado e selecione **Trust certificate**.

- Para criar unidades de hospedagem a partir de uma conexão de host existente, selecione **Use an existing Connection** e, em seguida, escolha a conexão relevante.

3. Na página **Namespace Selection**, selecione um namespace para esta conexão.
4. Na página **Seleção de Armazenamento**, selecione pelo menos um dispositivo de armazenamento para cada tipo de dados suportado antes de prosseguir para a próxima página do assistente. Para obter mais informações sobre a seleção de armazenamento, consulte Armazenamento do host.
5. Na página **Rede**, insira um nome para os recursos. Esse nome aparece no Studio para identificar a combinação de armazenamento e rede associada à conexão. Selecione uma ou mais redes que as VMs usarão.
6. Na página **Resumo**, verifique os detalhes e clique em **Concluir**.

Criar unidades de hospedagem usando PowerShell

Ao criar uma unidade de hospedagem usando o comando PowerShell, forneça as seguintes informações:

- Um nome de conexão de hospedagem
- Um nome de unidade de hospedagem
- O nome do namespace de destino
- Um nome de StorageClasses
- Um nome de NetworkAttachmentDefinition

1. Abra a janela do PowerShell.
2. Execute `add-pssnapin citrix*`.
3. Execute comandos do PowerShell para criar a unidade de hospedagem. Por exemplo:

```
$HostingConnectionName = "OpenShiftConnectionName"

$HostingUnitName = "HostingUnitName"

$TargetNamespace = "TargetNamespaceName"

$StorageClassToUse = "YourStorageClassesName"

$NetworkAttachmentDefinition = "YourNetworkAttachmentDefinitionName"

New-HypStorage `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage") `

-StorageType "TemporaryStorage"

New-Item `

-CustomProperties "" `

-HypervisorConnectionName $HostingConnectionName `

-NetworkPath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$NetworkAttachmentDefinition.network") `

-Path @("XDHyp:\HostingUnits\$HostingUnitName") -RootPath "XDHyp:
\Connections\$HostingConnectionName\$TargetNamespace.namespace" `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage")
```

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas
- Para informações específicas do Red Hat OpenShift, consulte Criar um catálogo do Red Hat OpenShift

Mais informações

- Conexões e recursos
- Ambientes de virtualização do Red Hat OpenShift

Conexão com VMware

Criar e gerenciar conexões e recursos descreve os assistentes que criam uma conexão. As informações a seguir cobrem detalhes específicos dos ambientes de virtualização VMware.

> **Nota:**
>
> Antes de criar uma conexão com o VMware, você precisa primeiro concluir a configuração da sua conta VMware como um local de recurso. Consulte Ambientes de virtualização VMware.

Permissões necessárias

Crie uma conta de usuário VMware e uma ou mais funções VMware com um conjunto ou todas as permissões listadas neste artigo. Baseie a criação das funções no nível específico de granularidade exigido sobre as permissões do usuário para solicitar as várias operações do Citrix DaaS™. Para conceder as permissões específicas do usuário a qualquer momento, associe-as à função respectiva, no nível do data center no mínimo, com a opção **Propagar para filhos** selecionada. No entanto, para as permissões `StorageProfile` e uma permissão `Tags` específica, aplique as permissões no nível do Root vCenter Server, sem **Propagar para Filhos**. Consulte as notas em cada uma dessas tabelas.

As tabelas a seguir mostram os mapeamentos entre as operações do Citrix DaaS e as permissões mínimas necessárias do VMware.

Adicionar conexões e recursos

SDK	INTERFACE DO USUÁRIO
System. Anonymous, System. Read e System.View	Adicionado automaticamente. Pode usar a função somente leitura integrada.

Gerenciamento de energia

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Interact.PowerOff	**Máquina virtual > Interação > Desligar**
VirtualMachine.Interact.PowerOn	**Máquina virtual > Interação > Ligar**
VirtualMachine.Interact.Reset	**Máquina virtual > Interação > Redefinir**

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Interact.Suspend	**Máquina virtual > Interação > Suspender**
Datastore.Browse	**Datastore > Navegar no datastore**

Provisionar máquinas (Machine Creation Services™)

Para provisionar máquinas usando MCS, as seguintes permissões são obrigatórias:

SDK	INTERFACE DO USUÁRIO
Datastore.AllocateSpace	**Datastore > Alocar espaço**
Datastore.Browse	**Datastore > Navegar no datastore**
Datastore.FileManagement	**Datastore > Operações de arquivo de baixo nível**
Network.Assign	**Rede > Atribuir rede**
Resource.AssignVMToPool	**Recurso > Atribuir máquina virtual ao pool de recursos**
VirtualMachine.Config.AddExistingDisk	**Máquina virtual > Configuração > Adicionar disco existente**
VirtualMachine.Config.AddNewDisk	**Máquina virtual > Configuração > Adicionar novo disco**
Máquina virtual.Config.Adicionar ou remover dispositivo	**Máquina virtual > Configuração > Adicionar ou remover dispositivo**
VirtualMachine.Config.AdvancedConfig	**Máquina virtual > Configuração > Avançado**
VirtualMachine.Config.RemoveDisk	**Máquina virtual > Configuração > Remover disco**
VirtualMachine.Config.CPUCount	**Máquina virtual > Configuração > Alterar contagem de CPU**
VirtualMachine.Config.Memory	**Máquina virtual > Configuração > Alterar memória**

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Config.Settings	**Máquina virtual > Configuração > Alterar configurações**
VirtualMachine.Interact.PowerOff	**Máquina virtual > Interação > Desligar**
VirtualMachine.Interact.PowerOn	**Máquina virtual > Interação > Ligar**
VirtualMachine.Interact.Reset	**Máquina virtual > Interação > Redefinir**
VirtualMachine.Interact.Suspend	**Máquina virtual > Interação > Suspender**
VirtualMachine.Inventory.CreateFromExisting	**Máquina virtual > Inventário > Criar a partir de existente**
VirtualMachine.Inventory.Create	**Máquina virtual > Inventário > Criar novo**
VirtualMachine.Inventory.Delete	**Máquina virtual > Inventário > Remover**
VirtualMachine.Provisioning.Clone	**Máquina virtual > Provisionamento > Clonar máquina virtual**
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Atualização 2, vSphere 5.1, Atualização 1 e vSphere 6.x, Atualização 1: **Máquina virtual > Estado > Criar instantâneo**; vSphere 5.5: **Máquina virtual > Gerenciamento de instantâneos > Criar instantâneo**; vSphere 8.0: **Máquina virtual > Gerenciamento de instantâneos > Criar instantâneo**
VirtualMachine.Config.Rename	**Máquina virtual > Configuração > Renomear**

Atualização e reversão de imagem

SDK	INTERFACE DO USUÁRIO
Datastore.AllocateSpace	**Datastore > Alocar espaço**
Datastore.Browse	**Datastore > Navegar no datastore**

SDK	INTERFACE DO USUÁRIO
Datastore.FileManagement	**Datastore > Operações de arquivo de baixo nível**
Network.Assign	**Rede > Atribuir rede**
Resource.AssignVMToPool	**Recurso > Atribuir máquina virtual ao pool de recursos**
VirtualMachine.Config.AddExistingDisk	**Máquina virtual > Configuração > Adicionar disco existente**
VirtualMachine.Config.AddNewDisk	**Máquina virtual > Configuração > Adicionar novo disco**
VirtualMachine.Config.AdvancedConfig	**Máquina virtual > Configuração > Avançado**
VirtualMachine.Config.RemoveDisk	**Máquina virtual > Configuração > Remover disco**
VirtualMachine.Interact.PowerOff	**Máquina virtual > Interação > Desligar**
VirtualMachine.Interact.PowerOn	**Máquina virtual > Interação > Ligar**
VirtualMachine.Interact.Reset	**Máquina virtual > Interação > Redefinir**
VirtualMachine.Inventory.CreateFromExisting	**Máquina virtual > Inventário > Criar a partir de existente**
VirtualMachine.Inventory.Create	**Máquina virtual > Inventário > Criar novo**
VirtualMachine.Inventory.Delete	**Máquina virtual > Inventário > Remover**
VirtualMachine.Provisioning.Clone	**Máquina virtual > Provisionamento > Clonar máquina virtual**

Compartilhar imagens preparadas

Para compartilhar imagens preparadas entre diferentes conexões de hospedagem, as seguintes permissões são obrigatórias para a conexão de hospedagem de destino:

SDK	INTERFACE DO USUÁRIO
Datastore.AllocateSpace	**Datastore > Alocar espaço**
Network.Assign	**Rede > Atribuir rede**
Resource.AssignVMToPool	**Recurso > Atribuir máquina virtual ao pool de recursos**
VirtualMachine.Config.Adicionar ou remover dispositivo	**Máquina virtual > Configuração > Adicionar ou remover dispositivo**
VirtualMachine.Config.RemoverDisco	**Máquina virtual > Configuração > Remover disco**
VirtualMachine.Config.Configurações	**Máquina virtual > Configuração > Alterar configurações**
VirtualMachine.Inventory.Registrar	**Máquina virtual > Inventário > Registrar**
VirtualMachine.Inventory.Excluir	**Máquina virtual > Inventário > Remover**
VirtualMachine.Provisioning.MarcarComoModelo	**Máquina virtual > Provisionamento > Marcar como modelo**
VirtualMachine.Provisioning.MarcarComoVM	**Máquina virtual > Provisionamento > Marcar como máquina virtual**
Host.Config.Rede	**Host > Configuração > Configuração de rede**

Excluir máquinas provisionadas

SDK	INTERFACE DO USUÁRIO
Datastore.Browse	**Datastore > Navegar no datastore**
Datastore.FileManagement	**Datastore > Operações de arquivo de baixo nível**
VirtualMachine.Config.RemoveDisk	**Máquina virtual > Configuração > Remover disco**
VirtualMachine.Interact.PowerOff	**Máquina virtual > Interação > Desligar**

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Inventory.Delete	**Máquina virtual > Inventário > Remover**

Perfil de Armazenamento

Para visualizar, criar ou excluir políticas de armazenamento durante a criação de catálogos em um datastore vSAN ou vVol, as seguintes permissões são obrigatórias:

SDK	INTERFACE DO USUÁRIO
StorageProfile.Update	**ARMAZENAMENTO ORIENTADO POR PERFIL > Atualizar armazenamento orientado por perfil**. Para vSphere 8: **Políticas de armazenamento de VM > Atualizar políticas de armazenamento de VM**
StorageProfile.View	**ARMAZENAMENTO ORIENTADO POR PERFIL > Visualizar armazenamento orientado por perfil**. Para vSphere 8: **Políticas de armazenamento de VM > Visualizar políticas de armazenamento de VM**

Nota:

Aplique as permissões de perfil de armazenamento no nível do Root vCenter Server, sem **Propagar para Filhos**.

Tags e Atributos Personalizados

Tags e atributos personalizados permitem anexar metadados às VMs criadas no inventário do vSphere e facilitam a pesquisa e filtragem desses objetos. Para criar, editar, atribuir e excluir tags ou categorias, as seguintes permissões são obrigatórias:

SDK	INTERFACE DO USUÁRIO
InventoryService.Tagging.CreateTag	**Marcação vSphere > Criar Marcação vSphere**

SDK	INTERFACE DO USUÁRIO
InventoryService.Tagging.CreateCategory	**vSphere Tagging > Criar Categoria de Tag vSphere**
InventoryService.Tagging.EditTag	**vSphere Tagging > Editar Tag vSphere**
InventoryService.Tagging.EditCategory	**vSphere Tagging > Editar Categoria de Tag vSphere**
InventoryService.Tagging.DeleteTag	**vSphere Tagging > Excluir Tag vSphere**
InventoryService.Tagging.DeleteCategory	**vSphere Tagging > Excluir Categoria de Tag vSphere**
InventoryService.Tagging.AttachTag	**vSphere Tagging > Atribuir ou Desatribuir Tag vSphere**
InventoryService.Tagging.ObjectAttachable	**vSphere Tagging > Atribuir ou Desatribuir Tag vSphere em Objeto**
Global.ManageCustomFields	**Global > Gerenciar atributos personalizados**
Global.SetCustomField	**Global > Definir atributo personalizado**

Nota:

- Quando o MCS cria um catálogo de máquinas, ele marca as VMs de destino com tags de nome especiais. Essas tags diferenciam a imagem mestre das VMs criadas pelo MCS e impedem o uso de VMs criadas pelo MCS para preparação de imagem. Você pode identificar a diferença pelo valor do atributo `XdProvisioned` no vCenter. O atributo é definido como **True** se o MCS criar VMs.
- Aplique a permissão `InventoryService.Tagging.AttachTag` no nível do Servidor vCenter Raiz, sem **Propagar para Filhos**.

Operações criptográficas

Os privilégios de operações criptográficas controlam quem pode realizar qual tipo de operação criptográfica em qual tipo de objeto. O vSphere Native Key Provider usa os privilégios `Cryptographer.*`. As seguintes permissões mínimas são necessárias para operações criptográficas:

Nota:

Essas permissões são necessárias para criar catálogos de máquinas MCS com VM equipada com vTPM.

SDK	INTERFACE DO USUÁRIO
Cryptographer.Access	**Privilégios > Todos os Privilégios > Operações criptográficas > Acesso Direto**
Cryptographer.AddDisk	**Privilégios > Todos os Privilégios > Operações criptográficas > Adicionar disco**
Cryptographer.Clone	**Privilégios > Todos os Privilégios > Operações criptográficas > Clonar**
Cryptographer.Encrypt	**Privilégios > Todos os Privilégios > Operações criptográficas > Criptografar**
Cryptographer.EncryptNew	**Privilégios > Todos os Privilégios > Operações criptográficas > Criptografar novo**
Cryptographer.Decrypt	**Privilégios > Todos os Privilégios > Operações criptográficas > Descriptografar**
Cryptographer.Migrate	**Privilégios > Todos os Privilégios > Operações criptográficas > Migrar**

SDK	INTERFACE DO USUÁRIO
Cryptographer.ReadKeyServersInfo	**Privilégios > Todos os Privilégios > Operações criptográficas > Ler informações do KMS**

Provisionar máquinas (Citrix Provisioning™)

Essas permissões para clonar e implantar um modelo são necessárias para provisionar VMs usando o Assistente de Configuração do Citrix Virtual Apps and Desktops™ e o Assistente de Exportação de Dispositivos através do console do Citrix Provisioning. Defina as permissões ao criar uma conexão de hospedagem. Você precisa de todas as permissões de Provisionar máquinas (Machine Creation Services) e as seguintes.

SDK	INTERFACE DO USUÁRIO
VirtualMachine.Config.AddRemoveDevice	**Máquina virtual > Configuração > Adicionar ou remover dispositivo**
VirtualMachine.Config.CPUCount	**Máquina virtual > Configuração > Alterar contagem de CPU**
VirtualMachine.Config.Memory	**Máquina virtual > Configuração > Memória**
VirtualMachine.Config.Settings	**Máquina virtual > Configuração > Configurações**
VirtualMachine.Provisioning.CloneTemplate	**Máquina virtual > Provisionamento > Clonar modelo**
VirtualMachine.Provisioning.DeployTemplate	**Máquina virtual > Provisionamento > Implantar modelo**
VApp.Export	**vApp > Exportar**

Nota:

O `VApp.Export` é necessário para criar catálogos de máquinas MCS usando perfil de máquina.

Protegendo conexões com o ambiente VMware

Usar conexões `HTTPS/SSL` com o vCenter exige que a conexão seja confiável para o Citrix DaaS.

Existem duas opções:

- (Recomendado) O banco de dados do Citrix DaaS tem a impressão digital SSL instalada. Essa impressão digital é usada pelo Citrix DaaS em cada Cloud Connector para confiar nas conexões com o vCenter.
- (Alternativa) Cada Cloud Connector confia no certificado do vCenter, e os serviços no Cloud Connector reutilizam essa confiança. Essa confiança pode vir de:
  - Certificado do vCenter, emitido pela Autoridade Certificadora e confiável para o Windows, resultando em confiança estabelecida entre Windows e vCenter.
  - Certificado do vCenter instalado no Windows, resultando em confiança estabelecida entre Windows e vCenter.OT

> **Nota:**
>
> O certificado do vCenter e a impressão digital SSL do VMware não são necessários para o VMware Cloud e suas soluções parceiras.

Impressão digital SSL do VMware

O recurso de impressão digital SSL do VMware aborda um erro frequentemente relatado ao criar uma conexão de host com um hipervisor VMware vSphere. Anteriormente, os administradores tinham que criar manualmente uma relação de confiança entre os Delivery Controllers gerenciados pelo Citrix no Site e o certificado do hipervisor antes de criar uma conexão. O recurso de impressão digital SSL do VMware remove essa exigência manual: a impressão digital do certificado não confiável é armazenada no banco de dados do Site para que o hipervisor possa ser continuamente identificado como confiável pelo Citrix DaaS, mesmo que não pelos Controllers.

Ao criar uma conexão de host vSphere, uma caixa de diálogo permite visualizar o certificado da máquina à qual você está se conectando. Você pode então escolher se deseja confiar nele.

O thumbprint SSL do VMware pode ser atualizado posteriormente usando o PowerShell SDK

```
Set-Item -LiteralPath "<FullPath_to_connection>" -username $cred.username
```

`-Securepassword $cred.password -SslThumbprint "<New ThumbPrint>" -hypervisorAddress <vcenter URL>`.

> **Dica:**
>
> O thumbprint do certificado deve ser escrito em letras maiúsculas.

Obter e importar um certificado

Para proteger as comunicações do vSphere, a Citrix® recomenda que você use HTTPS em vez de HTTP. HTTPS requer certificados digitais. A Citrix recomenda que você use um certificado digital emitido por uma autoridade de certificação de acordo com a política de segurança da sua organização.

Se você não puder usar um certificado digital emitido por uma autoridade de certificação, e a política de segurança da sua organização permitir, você pode usar o certificado autoassinado instalado no VMware. Adicione o certificado do VMware vCenter a cada Cloud Connector.

1. Adicione o nome de domínio totalmente qualificado (FQDN) do computador que executa o vCenter Server ao arquivo host nesse servidor, localizado em %SystemRoot%/WINDOWS/system32/Drivers/etc/. Esta etapa é necessária apenas se o FQDN do computador que executa o vCenter Server ainda não estiver presente no sistema de nomes de domínio.
2. Obtenha o certificado do vCenter usando qualquer um dos três métodos a seguir:

   Do servidor vCenter:

   a. Copie o arquivo rui.crt do servidor vCenter para um local acessível em seus Cloud Connectors.
   b. No Cloud Connector, navegar até o local do certificado exportado e abra o arquivo rui.crt.

   Baixe o certificado usando um navegador da web: Se você estiver usando o Internet Explorer, dependendo da sua conta de usuário, você deve clicar com o botão direito do mouse no Internet Explorer e escolher **Executar como administrador** para baixar ou instalar o certificado.

   a. Abra seu navegador da web e faça uma conexão web segura com o servidor vCenter (por exemplo `<https://server1.domain1.com>`).
   b. Aceite os avisos de segurança.
   c. Clique na barra de endereço que exibe o erro de certificado.

d. Clique em **O certificado não é válido** e, em seguida, clique na guia **Detalhes**.

e. Clique em **Exportar..**

f. Salve o certificado exportado.

g. navegar até o local do certificado exportado e abra o arquivo .CER.

Importar diretamente do Internet Explorer executado como administrador:

a. Abra seu navegador da web e faça uma conexão web segura com o servidor vCenter (por exemplo, `<https://server1.domain1.com>`).

b. Aceite os avisos de segurança.

c. Clique na barra de endereços que exibe o erro de certificado.

d. Visualize o certificado.

3. Importe o certificado para o armazenamento de certificados em cada Cloud Connector.

a. Clique em **Instalar certificado**, selecione **Máquina Local** e, em seguida, clique em **Avançar**.

b. Selecione **Colocar todos os certificados no seguinte armazenamento** e, em seguida, clique em **Procurar**. Em uma versão posterior compatível: Selecione **Pessoas Confiáveis** e, em seguida, clique em **OK**. Clique em **Avançar** e, em seguida, clique em **Concluir**.

> **Importante:**
>
> Se você alterar o nome do servidor vSphere após a instalação, você deve gerar um novo certificado autoassinado nesse servidor antes de importar o novo certificado.

Próximos passos

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas do VMware, consulte Criar um catálogo VMware.

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização VMware.
- Soluções de nuvem e parceiros VMware

Conexão com a nuvem VMware e soluções de parceiros

Após configurar cluster Azure VMware Solution (AVS), Google Cloud VMware Engine e VMware cloud on AWS, crie as conexões. Consulte Conexão com ambientes de virtualização VMware para criar conexões.

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para informações específicas do VMware, consulte Criar um catálogo VMware.

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização VMware.
- Nuvem VMware e soluções de parceiros

Conexão com XenServer®

Criar e gerenciar conexões e recursos fornece instruções detalhadas usando o assistente para criar uma conexão. Antes de estabelecer uma conexão com o XenServer (anteriormente Citrix Hypervisor), você precisa primeiro concluir a configuração do seu XenServer como um host. Consulte Adicionar um tipo de recurso ou ativar um domínio não utilizado no Citrix Cloud.

Criar uma conexão com o XenServer

Ao criar uma conexão com o XenServer, você deve fornecer as credenciais para um Administrador de Energia de Máquina Virtual (VM Power Admin) ou um usuário de nível superior.

A Citrix recomenda usar HTTPS para proteger as comunicações com o XenServer. Para usar HTTPS, você deve substituir o certificado TLS padrão instalado no XenServer. Para obter mais informações, consulte Instalar um certificado TLS em seu servidor.

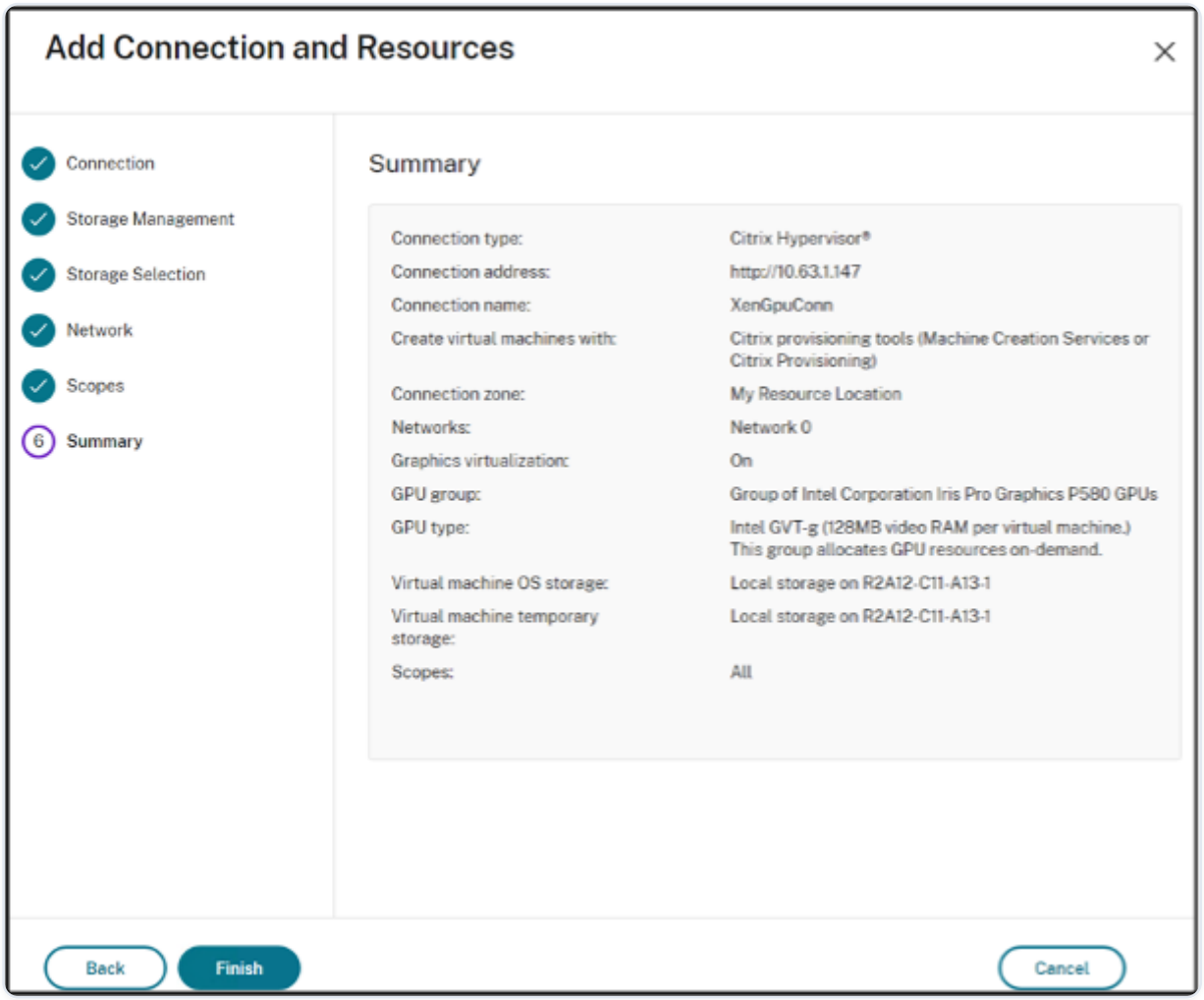
Você pode configurar a alta disponibilidade se ela estiver habilitada no servidor XenServer. A Citrix® recomenda que você selecione todos os servidores no pool (em **Editar Alta Disponibilidade**) para permitir a comunicação com o servidor XenServer caso o mestre do pool falhe.

> **Nota:**

> Se você estiver usando HTTPS e quiser configurar servidores de alta disponibilidade, agora você pode instalar um certificado curinga para todos os servidores em um pool.

> Ao usar armazenamento local em um ou mais hosts XenServer para armazenamento temporário de dados, certifique-se de que cada local de armazenamento no pool tenha um nome exclusivo. (Para alterar um nome no XenCenter®, clique com o botão direito do mouse no armazenamento e edite a propriedade do nome.)

Se você se conectar ao XenServer que suporta vGPU, poderá verificar o grupo de GPU e o tipo de GPU na página **Resumo** do assistente para criar uma conexão.



Usar IntelliCache™ para conexões XenServer

Usando o IntelliCache, as implantações de VDI hospedadas são mais econômicas porque você pode usar uma combinação de armazenamento compartilhado e armazenamento local. Isso melhora o desempenho e reduz o tráfego de rede. O armazenamento local armazena em cache a imagem mestre do armazenamento compartilhado, o que reduz a quantidade de leituras no armazenamento compartilhado. Para desktops compartilhados, as gravações nos discos de

diferenciação são gravadas no armazenamento local no host e não no armazenamento compartilhado.

As considerações importantes são:

- O armazenamento compartilhado deve ser NFS ao usar o IntelliCache.
- A Citrix recomenda que você use um dispositivo de armazenamento local de alto desempenho para garantir a transferência de dados mais rápida possível.

Para usar o IntelliCache, habilite o IntelliCache conforme detalhado:

- Ao instalar o XenServer, selecione **Enable thin provisioning**. Consulte Instalar o host XenServer para obter informações sobre como instalar o host XenServer a partir de mídia local. A Citrix não oferece suporte a pools mistos de servidores com alguns servidores que têm o IntelliCache habilitado e outros que não têm o IntelliCache habilitado.
- No Citrix DaaS™, o IntelliCache é desabilitado por padrão. Você pode alterar a configuração somente ao criar uma conexão XenServer. Não é possível desabilitar o IntelliCache posteriormente. Ao criar uma conexão XenServer:
  - Selecione **Compartilhado** como o tipo de armazenamento.
  - Marque a caixa de seleção **Usar IntelliCache**.

Consulte IntelliCache para obter mais informações.

Permissões necessárias do XenServer

As permissões do XenServer são baseadas em função (RBAC). O recurso Controle de Acesso Baseado em Função (RBAC) no XenServer permite atribuir usuários, funções e permissões para controlar quem tem acesso ao seu XenServer e quais ações eles podem executar. O sistema RBAC do XenServer mapeia um usuário (ou um grupo de usuários) para funções definidas (um conjunto nomeado de permissões). As funções têm permissões XenServer associadas para executar certas operações.

Para obter mais informações, consulte Controle de acesso baseado em função.

A hierarquia de funções, em ordem crescente de permissões, é: Somente Leitura → Operador de VM → Administrador de VM → Administrador de Energia de VM → Operador de Pool → Administrador de Pool.

A seção a seguir resume a função mínima necessária para cada tarefa de provisionamento.

Criando uma conexão de host

TAREFA	FUNÇÃO MÍNIMA NECESSÁRIA
Adicionar uma conexão de host usando as informações obtidas do XenServer	Somente leitura
Visualizar usuários e suas funções atribuídas	Somente leitura

Gerenciamento de energia de VMs

TAREFA	FUNÇÃO MÍNIMA NECESSÁRIA
Ligar ou desligar as VMs	Operador de VM

Criar, atualizar ou excluir VMs

TAREFA	FUNÇÃO MÍNIMA NECESSÁRIA
Adicionar ou remover VMs de agendamentos de snapshots existentes	Administrador de energia de VM
Adicionar, modificar, excluir agendamentos de snapshots	Operador de Pool
Publicar imagem mestre	Operador de Pool (Requer bloqueio de porta de switch)
Criar um catálogo de máquinas	Operador de Pool: Requer bloqueio de porta de switch
Adicionar ou remover VMs (VMs não habilitadas para GPU)	Administrador de VM
Adicionar ou remover VMs (VMs habilitadas para GPU)	Operador de Pool
Adicionar, remover ou configurar disco virtual ou dispositivos de CD	Administrador de VM
Gerenciar Tags	Operador de VM

Para obter mais informações sobre funções e permissões RBAC, consulte funções e permissões RBAC.

Para obter informações sobre o bloqueio de porta de switch, consulte Usar bloqueio de porta de switch.

Onde ir em seguida

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas do XenServer, consulte Criar um catálogo do XenServer.

Mais informações

- Criar e gerenciar conexões e recursos
- Ambientes de virtualização XenServer

Contas de serviço

Uma conta de serviço é um contêiner para credenciais armazenadas, que é configurada e usada para realizar operações relacionadas à identidade da máquina sem interação do usuário. Crie a conta de serviço antes das operações que exigem permissões para o gerenciamento de identidade da máquina.

Você pode configurar um catálogo de máquinas MCS para usar uma conta de serviço para:

- criar ou excluir contas de computador no Active Directory sem precisar inserir as credenciais de domínio todas as vezes.
- gerenciar dispositivos obsoletos ingressados no Microsoft Entra ou registrados no Microsoft Intune sem excluí-los manualmente através do portal do Microsoft Entra ID ou Intune.

Tipos de conta de serviço suportados

A Citrix® permite a criação de dois tipos de contas de serviço com base no tipo de provedor de identidade.

TIPO DE PROVEDOR DE IDENTIDADE	DESCRIÇÃO	CREDENCIAIS
Conta de serviço do Active Directory local	Gerencia catálogos de máquinas e contas de computador sem precisar inserir as credenciais de domínio todas as vezes.	Nome de usuário e senha de contas de usuário do Active Directory local.

TIPO DE PROVEDOR DE IDENTIDADE	DESCRIÇÃO	CREDENCIAIS
Conta de serviço do Microsoft Entra	Combina um principal de serviço com capacidade de gerenciamento de dispositivos para conceder permissões para o gerenciamento de dispositivos.	ID do aplicativo e segredo de um principal de serviço do Microsoft Entra.

Proteção de credenciais

A Citrix armazena as credenciais das contas de serviço no banco de dados do site do cliente. No DaaS, o banco de dados do site é um banco de dados por locatário (cliente), que é acessível apenas pelos serviços em execução para o cliente.

As seguintes ações também são aplicadas para proteger as credenciais armazenadas:

- As credenciais são criptografadas usando criptografia **AES 256** antes de serem armazenadas no banco de dados.
- A chave de criptografia é gerada por site e armazenada localmente no Delivery Controller™, que só pode ser acessada pelos serviços dedicados ao cliente.
- A conexão com o banco de dados é criptografada usando o protocolo TLS 1.2.

Contas de serviço do Active Directory no local

Uma conta de serviço do Active Directory no local é um contêiner para armazenar o nome de usuário e a senha de uma conta de usuário de domínio privilegiada. A conta de usuário deve ter permissões suficientes para gerenciar contas de computador em um Active Directory. O Machine Creation Service pode usar essa conta de serviço para realizar operações relacionadas a contas de computador sem inserir as credenciais de domínio todas as vezes.

Criar uma conta de serviço do Active Directory no local

Crie uma conta de serviço do Active Directory no local usando o Studio ou o PowerShell.

Pré-requisito

Para criar uma conta de serviço do Active Directory no local, certifique-se de concluir a seguinte tarefa:

- Crie uma conta de usuário de domínio em seu Active Directory com permissões suficientes para criar, atualizar e excluir objetos de computador em seu Active Directory ou OUs específicas.

Usar o Studio

1. No bloco **DaaS**, clique em **Gerenciar**.
2. No painel esquerdo, selecione **Administradores**.
3. Na guia **Contas de Serviço**, clique em **Criar Conta de Serviço**.
4. Na página **Tipo de Identidade**, selecione **Active Directory no local**. Clique em **Avançar**.
5. Na página **Credenciais**, clique em **Inserir credenciais** para fornecer o nome de usuário e a senha de uma conta de usuário de domínio privilegiada que você deseja usar como conta de serviço.
6. Defina a data de expiração da senha ou deixe-a como nunca expira.
7. Selecione um ou mais escopos para esta conta de serviço.
8. Insira um nome amigável e uma descrição (opcional) para a conta de serviço.
9. Clique em **Concluir** para finalizar a criação.

Usar PowerShell

Você pode usar comandos PowerShell para criar um serviço do Active Directory local. Por exemplo:

```
$credential = ConvertTo-SecureString -String $password -AsPlainText -Force

New-AcctServiceAccount -IdentityProviderType ActiveDirectory
-IdentityProviderIdentifier test.local -AccountId test\svcacct_mcs
-AccountSecret $credential -SecretExpiryTime 2030/08/15 -DisplayName
'scvacct_mcs' -Description 'Service account for test.local'
```

Nota:

O `$password` é a senha correspondente para a conta de usuário de domínio fornecida.

Executar ações relacionadas à identidade de máquinas

Depois que um pool de identidades baseado em Active Directory ou Microsoft Entra híbrido é associado a uma conta de serviço, você pode realizar várias ações relacionadas à identidade de máquinas sem precisar inserir as credenciais de domínio.

- Para criar uma nova conta de identidade usando uma conta de serviço

```
New-AcctADAccount -IdentityPoolName MyPool -Count 2 -UseServiceAccount
```

- Para reparar as contas de identidade usando uma conta de serviço

```
Repair-AcctADAccount -ADAccountName "Domain\account","Domain\account2"
-UseServiceAccount
```

- Para remover contas de identidade usando uma conta de serviço

```
Remove-AcctADAccount -IdentityPoolName MyPool -RemovalOption Delete
-ADAccountName "Domain\account","domain\account2" -UserServiceAccount
```

Onde ir em seguida

- Para criar catálogos unidos ao Active Directory local, consulte Pool de identidades de máquina unida ao Active Directory local.
- Para gerenciar contas de serviço, consulte Gerenciar contas de serviço.

Contas de serviço do Microsoft Entra

Uma conta de serviço do Microsoft Entra é um contêiner para armazenar o ID do aplicativo e o segredo de um principal de serviço do Microsoft Entra, que possui permissões suficientes para gerenciar dispositivos ingressados no Microsoft Entra ou registrados no Microsoft Intune. O MCS pode usar essa conta de serviço para limpar automaticamente quaisquer dispositivos Microsoft Entra ou Microsoft Intune obsoletos gerados durante o ciclo de vida das máquinas provisionadas.

Permissões necessárias para um principal de serviço do Microsoft Entra

As permissões necessárias para um principal de serviço do Microsoft Entra usado por uma conta de serviço dependem dos recursos habilitados para a conta de serviço.

- Para a conta de serviço com capacidade de gerenciamento de dispositivos ingressados no Microsoft Entra, o principal de serviço do Microsoft Entra deve ter a permissão `Device.ReadWrite.All` em seu locatário do Microsoft Entra.
- Para a conta de serviço com capacidade de gerenciamento de dispositivos registrados no Microsoft Intune, o principal de serviço do Microsoft Entra deve ter a permissão `DeviceManagementManagedDevices.ReadWrite.All` em seu locatário do Microsoft Entra.
- Para a conta de serviço com capacidade de gerenciamento de grupo de segurança do Microsoft Entra, o principal de serviço do Microsoft Entra deve ter as permissões `Group.ReadWrite.All` e `GroupMember.ReadWrite.All` em seu locatário do Microsoft Entra.

Limitação

O controle de acesso baseado em função do Microsoft Entra não é atualmente suportado. Portanto, atribua as permissões do Microsoft Entra diretamente ao principal de serviço.

Criar uma conta de serviço do Microsoft Entra

Use o Studio ou o PowerShell para criar uma conta de serviço do Microsoft Entra.

Pré-requisito

Para criar uma conta de serviço do Microsoft Entra, certifique-se de concluir a seguinte tarefa:

- Crie um principal do Microsoft Entra em seu locatário do Microsoft Entra com permissões suficientes com base nos recursos que você deseja habilitar para a conta de serviço.

Usar o Studio

1. No bloco **DaaS**, clique em **Gerenciar**.
2. No painel esquerdo, selecione **Administradores**.
3. Na guia **Contas de Serviço**, clique em **Criar Conta de Serviço**.
4. Na página **Tipo de Identidade**, selecione **Microsoft Entra ID**. Uma nova opção para rotear o tráfego é habilitada.
    a. Marque a caixa de seleção **Roteie o tráfego por meio dos Citrix Cloud Connectors**.
    b. Selecione as zonas disponíveis para rotear o tráfego e clique em **Avançar**.
5. Na página **Credenciais**, insira o ID do locatário do Microsoft Entra, o ID do aplicativo e o segredo do cliente e defina a data de expiração da credencial.
6. Escolha os recursos para a conta de serviço.

7. Selecione um ou mais escopos para a conta de serviço.
8. Insira um nome amigável e uma descrição (opcional) para a conta de serviço.
9. Clique em **Concluir** para finalizar a criação.

Nota:

- O recurso de gerenciamento de dispositivos ingressados no Microsoft Entra é selecionado por padrão e você não pode desmarcá-lo.
- Para usar um aplicativo Microsoft Entra multilocatário, que é convidado para o seu locatário, o ID do locatário do Microsoft Entra que você inseriu deve ser o seu próprio ID de locatário, e não o ID do locatário inicial do aplicativo.

Usar PowerShell

Alternativamente, você pode usar comandos PowerShell para criar uma conta de serviço do Microsoft Entra. Por exemplo:

```
$tenantId = xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

$applicationId = xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

$applicationSecret = xxxxxxxxxxxxxxx

$credential = ConvertTo-SecureString -String $applicationSecret
-AsPlainText -Force



New-AcctServiceAccount -IdentityProviderType AzureAD
-IdentityProviderIdentifier $tenantId -AccountId $applicationId
-AccountSecret $credential -SecretExpiryTime 2030/08/15 -Capabilities
@("AzureADDeviceManagement","IntuneDeviceManagement") -DisplayName
'MyApplication' -Description 'Service account for Microsoft Entra tenant'
```

Migrar o gerenciamento de dispositivos unidos ao Microsoft Entra para a conta de serviço

Anteriormente, a Citrix® fornecia uma opção para habilitar o gerenciamento de dispositivos unidos ao Microsoft Entra ao criar ou editar uma conexão de hospedagem com o Microsoft Azure Resource Manager. O MCS usava as permissões do principal de serviço do Microsoft Entra (SPN de provisionamento) armazenadas junto com a conexão de hospedagem para gerenciar o dispositivo unido ao Microsoft Entra obsoleto. Com as contas de serviço, você pode usar um principal de serviço do Microsoft Entra dedicado (SPN de gerenciamento de identidade) armazenado junto com uma conta de serviço para gerenciar dispositivos unidos ao Microsoft Entra ou registrados no Microsoft Intune.

A Citrix recomenda migrar do gerenciamento de dispositivos baseado em conexão de hospedagem para o gerenciamento de dispositivos baseado em conta de serviço para separar a responsabilidade do SPN de provisionamento e do SPN de gerenciamento de identidade.

Para quaisquer conexões de hospedagem existentes que já estejam habilitadas com o gerenciamento de dispositivos unidos ao Microsoft Entra, você pode desativá-lo da seguinte forma:

1. No Studio, selecione **Hospedagem** no painel esquerdo.
2. Selecione a conexão e, em seguida, selecione **Editar Conexão** na barra de ações.
3. Na página **Propriedades da Conexão**, desmarque a caixa de seleção **Habilitar gerenciamento de dispositivos unidos ao Microsoft Entra**.
4. Clique em **Salvar** para aplicar as alterações.

> **Nota:**
>
> Atualmente, você não pode habilitar o gerenciamento de dispositivos unidos ao Microsoft Entra ao criar uma nova conexão de hospedagem.

Encaminhar o tráfego de gerenciamento de dispositivos Microsoft Entra e gerenciamento de grupos de segurança

Crie e modifique uma conta de serviço do Microsoft Entra para rotear o tráfego de gerenciamento de dispositivos Microsoft Entra e gerenciamento de grupos de segurança do Delivery Controller para o Microsoft Entra ID através do Citrix Cloud Connector.

Inclua a seguinte propriedade personalizada ao criar ou modificar uma conta de serviço do Microsoft Entra:

`CustomProperties: {"ProxyHypervisorTrafficThroughConnector":true,"ZoneUid":["<zone uid>"]}`

> **Observação:**
>
> O `$ZoneUid` é o Uid da zona (local do recurso) para onde o tráfego de rede deve ser roteado. Obtenha o Uid do comando `Get-ConfigZone`.
>
> Por exemplo:

- Para criar uma nova conta de serviço do Microsoft Entra:

```
$tenantId = xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

$applicationId = xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

$applicationSecret = xxxxxxxxxxxxxxx

$SecureString = ConvertTo-SecureString -String "Secretstring"
-AsPlainText -Force

New-AcctServiceAccount -IdentityProviderType AzureAD
-IdentityProviderIdentifier "<Identity provider ID>" -AccountId
"<Account ID>" -AccountSecret $SecureString -SecretExpiryTime <yyyy-mm-
dd>  -Capabilities
@("AzureADDeviceManagement","IntuneDeviceManagement") -DisplayName
"<Display name>" -CustomProperties
'{"ProxyHypervisorTrafficThroughConnector":true,"ZoneUid":["<Zone
UID>"]}'
```

- Para modificar uma conta de serviço do Microsoft Entra existente:

```
Set-AcctServiceAccount -ServiceAccountUid $serviceAccountUid
-CustomProperties
'{"ProxyHypervisorTrafficThroughConnector":true,"ZoneUid":[$ZoneUid]}'
```

Próximos passos

- Para criar catálogos unidos ao Microsoft Entra, consulte Pool de identidades de identidade de máquina unida ao Microsoft Entra.
- Para gerenciar contas de serviço, consulte Gerenciar contas de serviço.

Gerenciar contas de serviço

Gerenciar contas de serviço é um aspecto crítico para garantir que elas permaneçam em um estado saudável e que suas credenciais estejam atualizadas. Este artigo descreve as etapas para visualizar, renomear, editar, testar e excluir uma conta de serviço.

Visualizar detalhes da conta de serviço

1. No bloco **DaaS**, clique em **Gerenciar**.
2. No painel esquerdo, selecione **Administradores**.
3. Selecione a guia **Contas de Serviço**.
4. Selecione uma conta de serviço e visualize seus detalhes no painel inferior. Veja as propriedades de cada conta de serviço, juntamente com seus catálogos de máquinas associados e dicas de solução de problemas no painel inferior.

Ícones de erro ou aviso aparecem ao lado de uma conta de serviço se:

- a conta de serviço estiver em um estado não saudável.
- a credencial de uma conta de serviço estiver perto de expirar.

A guia **Solução de Problemas** fornece informações para diagnosticar e corrigir os problemas.

> **Nota:**

> Após corrigir os problemas, faça um teste de conta de serviço para atualizar o status. Para obter mais informações, consulte Testar uma conta de serviço.

Renomear uma conta de serviço

1. No bloco **DaaS**, clique em **Gerenciar**.
2. No painel esquerdo, selecione **Administradores**.
3. Selecione a guia **Contas de Serviço**.
4. Selecione uma conta de serviço e clique em **Renomear**.

Editar uma conta de serviço

1. No bloco **DaaS**, clique em **Gerenciar**.
2. No painel esquerdo, selecione **Administradores**.
3. Selecione a guia **Contas de Serviço**.
4. Selecione uma conta de serviço e clique em **Editar**.

Testar uma conta de serviço

1. No bloco **DaaS**, clique em **Gerenciar**.
2. No painel esquerdo, selecione **Administradores**.
3. Selecione a guia **Contas de Serviço**.
4. Selecione uma conta de serviço e clique em **Testar Conta de Serviço**.

- Para uma conta de serviço do Active Directory local, as credenciais são verificadas durante o teste.
- Para uma conta de serviço do Microsoft Entra, o ID do aplicativo e o segredo, juntamente com as permissões necessárias, são verificados durante o teste.

Identifique e corrija os problemas de acordo com as recomendações. A guia **Solução de problemas** fornece informações para diagnosticar e corrigir os problemas. Após corrigir os problemas, teste a conta de serviço.

Excluir uma conta de serviço

Antes de excluir uma conta de serviço, certifique-se de que a conta de serviço não seja usada por nenhum catálogo de máquinas MCS.

1. No bloco **DaaS**, clique em **Gerenciar**.
2. No painel esquerdo, selecione **Administradores**.
3. Selecione a guia **Contas de Serviço**.
4. Selecione uma conta de serviço e clique em **Excluir**.

Gerenciamento de imagens

Introdução

O processo de criação ou atualização do catálogo MCS tem duas fases:

- Masterização: uma imagem de origem é convertida em uma imagem publicada
- Clonagem: novas VMs são criadas a partir da imagem publicada

Com a funcionalidade de gerenciamento de imagens, o MCS separa a fase de masterização do fluxo de trabalho geral de provisionamento.

Você pode preparar várias versões de imagem MCS (Imagem Preparada) a partir de uma única imagem de origem e usá-las em vários catálogos de máquinas MCS diferentes. Você também pode compartilhar versões de imagens preparadas entre unidades de hospedagem. Essa implementação reduz significativamente os custos de armazenamento e tempo, e simplifica o processo de implantação de VM e atualização de imagem.

Os benefícios de usar essa funcionalidade de gerenciamento de imagens são:

- Gerar imagens preparadas com antecedência sem criar um catálogo.
- Reutilizar imagens preparadas em vários cenários, como criação e atualização de um catálogo.
- Reduzir significativamente o tempo de criação ou atualização do catálogo.
- Compartilhar versões de imagens preparadas entre unidades de hospedagem:
    - Para Azure, Nutanix AHV Prism Central e VMware, as versões de imagem podem ser compartilhadas entre conexões de host do mesmo tipo de conexão.
    - Para Amazon WorkSpaces Core Managed Instances, as versões de imagem podem ser compartilhadas entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região AWS ou em regiões diferentes.
    - Para AWS EC2, as versões de imagem podem ser compartilhadas entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região AWS.
    - Para XenServer, as versões de imagem só podem ser compartilhadas entre unidades de hospedagem dentro da mesma conexão de host.

Nota:

- Este recurso é atualmente aplicável a instâncias gerenciadas do Amazon WorkSpaces Core, AWS EC2, Azure, Nutanix AHV Prism Central, Red Hat OpenShift, virtualização VMware e ambientes XenServer.

> - Você pode criar um catálogo de máquinas MCS sem usar imagens preparadas. Nesse caso, você não pode obter os benefícios do recurso. No entanto, para instâncias gerenciadas do Amazon WorkSpaces Core, crie o catálogo MCS usando apenas uma versão de imagem preparada. Você não pode criar o catálogo usando uma imagem mestre diretamente.

Casos de uso

Alguns dos casos de uso da funcionalidade de gerenciamento de imagens são:

- *Gerenciamento de versões*: As versões de imagem permitem que você:
  - gerenciar diferentes iterações ou atualizações de uma imagem específica.
  - manter várias versões de uma imagem para diferentes propósitos.
- *Agrupamento lógico*: Você pode criar várias definições de imagem para:
  - agrupar logicamente versões de imagem com base em vários critérios, como projeto, departamento ou tipo de aplicativo e desktop.
  - gerenciar imagens de forma mais eficiente dentro de uma organização.
- *Compartilhamento de imagem*: Você pode compartilhar versões de imagem preparadas entre unidades de hospedagem dentro de conexões de host do mesmo tipo de conexão para:
  - garantir a consistência e uniformidade das imagens em diferentes unidades de hospedagem.

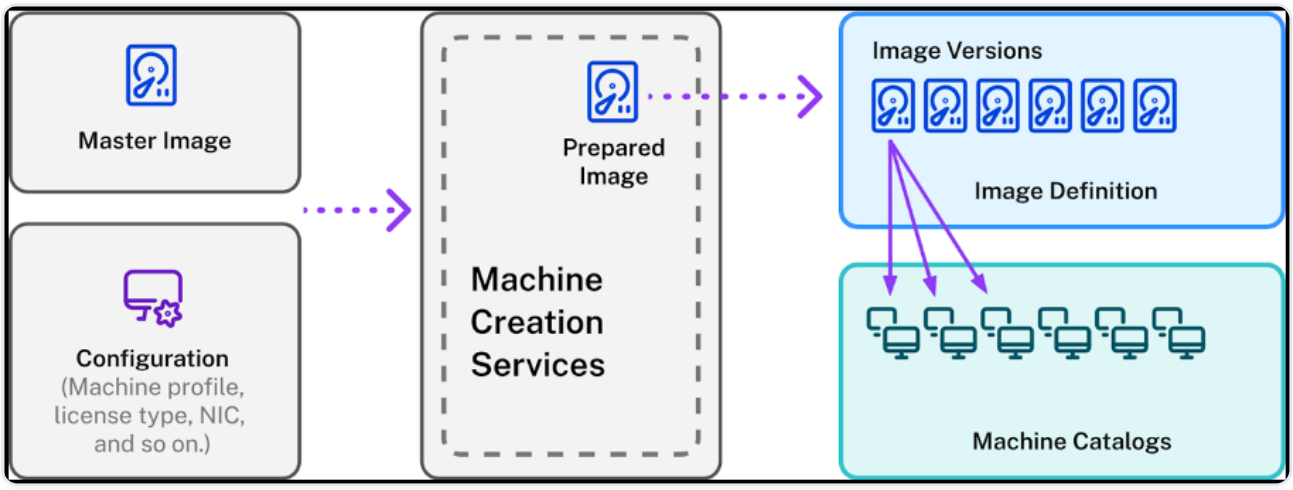
O que é uma imagem preparada?

Com a funcionalidade de gerenciamento de imagens, o MCS desvincula a fase de masterização do fluxo de trabalho geral de criação ou atualização de catálogo e divide o processo em duas etapas:

1. Crie imagens preparadas a partir de uma única imagem de origem.
2. Use a imagem preparada para criar ou atualizar um catálogo de máquinas MCS.

Você pode criar as imagens preparadas com antecedência. Você pode usar uma única imagem preparada para criar ou atualizar vários catálogos de máquinas provisionados pelo MCS.

Entenda como uma imagem preparada é usada em vários catálogos de máquinas MCS ao usar o Studio:



Definição de imagem: As definições de imagem são um agrupamento lógico de versões de uma imagem. A definição de imagem contém informações sobre:

- por que a imagem foi criada
- para qual SO ela se destina
- outras informações sobre o uso da imagem.

Um catálogo não é criado a partir de uma definição de imagem, mas a partir das versões de imagem que são criadas com base na definição de imagem.

Versão da imagem: As versões da imagem gerenciam o versionamento para a definição da imagem. Uma definição de imagem pode ter várias versões de imagem. Use as versões da imagem como imagens preparadas para criar ou atualizar um catálogo.

- Para Azure e VMware, as versões de imagem podem ser compartilhadas entre conexões de host do mesmo tipo de conexão.
- Para instâncias gerenciadas do Amazon WorkSpaces Core, as versões de imagem podem ser compartilhadas entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região AWS ou em regiões diferentes.
- Para AWS EC2, as versões de imagem podem ser compartilhadas entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região AWS.
- Para XenServer, as versões de imagem só podem ser compartilhadas entre unidades de hospedagem dentro da mesma conexão de host.

Alternativamente, se você quiser usar comandos PowerShell para criar um esquema de provisionamento para criar ou atualizar um catálogo, então você deve criar uma especificação de

versão de imagem preparada baseada na especificação de versão de imagem mestre, conforme necessário para o seu ambiente.

- Para Azure, Nutanix AHV Prism Central e VMware, as versões de imagem podem ser compartilhadas entre conexões de host do mesmo tipo de conexão.
- Para Amazon WorkSpaces Core Managed Instances, as versões de imagem podem ser compartilhadas entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região AWS ou em regiões diferentes.
- Para AWS EC2, as versões de imagem podem ser compartilhadas entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região AWS.
- Para XenServer, as versões de imagem só podem ser compartilhadas entre unidades de hospedagem dentro da mesma conexão de host.

Requisito

- Para imagens mestre do Windows, apenas imagens VDA versão 2311 ou posterior são suportadas. O componente MCS/IO deve ser explicitamente selecionado e instalado. A ativação ou desativação da configuração de E/S do MCS deve ser determinada durante a criação ou atualização do catálogo de máquinas, pois não está ativada por padrão.

Limitações

Atualmente, o recurso não oferece suporte ao seguinte:

- Múltiplas NICs no Azure
- Recurso de disco de dados persistente
- Hibernação para multi-sessão
- Alteração do tipo de imagem
- Ao compartilhar a versão da imagem preparada entre unidades de hospedagem no Azure, os seguintes métodos de compartilhamento não são permitidos:
  - Compartilhar Diretamente
  - Compartilhar para a galeria da comunidade pública

Gerenciamento do ciclo de vida da imagem usando o Studio

O ciclo de vida da imagem ao usar o Studio é o seguinte:

1. Criar uma imagem preparada: Crie uma definição de imagem e sua versão inicial de imagem.
2. Crie versões de imagem a partir da versão inicial da imagem.
3. Se necessário, compartilhe uma versão de imagem com uma unidade de hospedagem em seu ambiente de virtualização.
4. Use uma versão de imagem como uma imagem preparada para criar catálogos.
5. Atualize um catálogo de máquinas com uma imagem preparada diferente.
6. Gerencie as definições e versões de imagem: Edite o nome e a descrição das versões de imagem, e a descrição de uma definição de imagem.
7. Excluir uma versão de imagem.
8. Excluir uma definição de imagem.

Alternativamente, você também pode gerenciar imagens usando o PowerShell. Consulte Gerenciamento do ciclo de vida da imagem usando o PowerShell.

Gerenciamento do ciclo de vida da imagem usando o PowerShell

Se você deseja usar comandos do PowerShell para criar um esquema de provisionamento, então você deve criar uma especificação de versão de imagem preparada com base na especificação de versão da imagem mestre, conforme necessário para o seu ambiente.

Especificação de versão de imagem mestre: Uma especificação de versão de imagem mestre é uma imagem específica adicionada ou criada sob uma versão de imagem. Você pode adicionar uma imagem existente no hipervisor como uma especificação de versão de imagem mestre ou criar uma especificação preparada com base na especificação mestre, conforme necessário para o seu ambiente. A especificação preparada pode ser usada para vários esquemas de provisionamento.

Você pode compartilhar especificações de versão de imagem entre unidades de hospedagem, dependendo do seu ambiente de virtualização:

- Em ambientes Azure, VMware e Amazon WorkSpaces Core Managed Instances, você pode compartilhar especificações de versão de imagem entre unidades de hospedagem, estejam elas nas mesmas ou em diferentes conexões de host do mesmo tipo de conexão. No Azure, o compartilhamento é feito usando o recurso de compartilhamento de disco do Azure Compute Gallery (ACG).
- Para AWS EC2, as versões de imagem podem ser compartilhadas entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região da AWS.

- No Nutanix AHV Prism Central e XenServer, você pode compartilhar especificações de versão de imagem apenas entre unidades de hospedagem dentro da mesma conexão de host.

O ciclo de vida de uma imagem ao usar comandos PowerShell é:

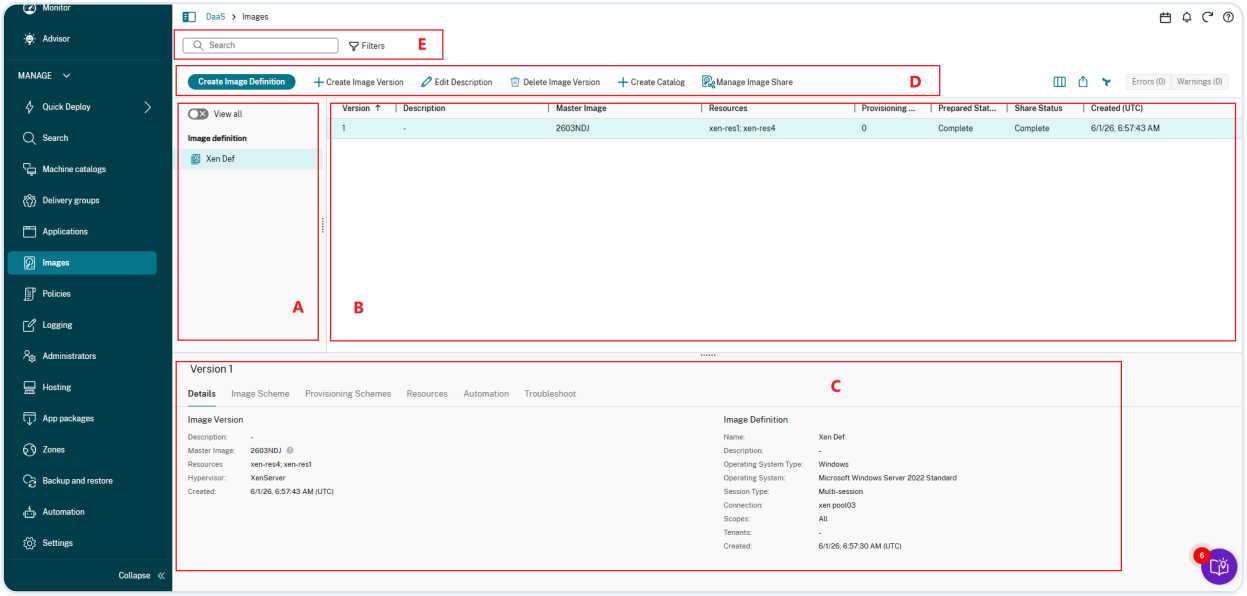
1. Criar uma imagem:
    a. Criar uma definição de imagem.
    b. Adicionar uma nova configuração para Definição de Imagem na conexão de hospedagem especificada.
    c. Criar uma versão de imagem.
    d. Adicionar uma especificação de versão de imagem mestre.
    e. Criar uma especificação de versão de imagem preparada.
2. Se necessário, compartilhe uma especificação de versão de imagem com outra unidade de hospedagem, seguindo as restrições de compartilhamento do seu ambiente de virtualização:
    - Para Azure e VMware, as versões de imagem podem ser compartilhadas entre conexões de host do mesmo tipo de conexão.
    - Para Amazon WorkSpaces Core Managed Instances, as versões de imagem podem ser compartilhadas entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região da AWS ou em regiões diferentes.
    - Para AWS EC2, as versões de imagem podem ser compartilhadas entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região da AWS.
    - Para XenServer, as versões de imagem só podem ser compartilhadas entre unidades de hospedagem dentro da mesma conexão de host.
3. Crie um catálogo de máquinas MCS usando uma especificação de versão de imagem preparada:
    a. Crie um catálogo de broker.
    b. Crie um pool de identidades.
    c. Crie um esquema de provisionamento com o parâmetro da especificação de versão de imagem preparada Uid usando o comando `New-ProvScheme`.
    d. Vincule o catálogo de broker ao esquema de provisionamento.
4. Crie VMs no catálogo de máquinas MCS.

5. Altere a especificação de versão de imagem preparada de um esquema de provisionamento usando o comando `Set-ProvScheme`.
6. Gerencie as definições e versões de imagem: Edite as versões de imagem e as definições de imagem.
7. Exclua um catálogo de máquinas MCS: A ordem de exclusão é: catálogo de máquinas > especificação de versão de imagem preparada compartilhada (se houver compartilhamento de imagem) > especificação de versão de imagem preparada > especificação de versão de imagem mestre > versão de imagem > configuração para definição de imagem na conexão de hospedagem especificada > definição de imagem. Antes de excluir a especificação de versão de imagem, certifique-se de que a especificação de versão de imagem preparada não esteja associada a nenhum catálogo de máquinas MCS.

Entender o nó Imagens

Use o nó **Imagens** para criar e gerenciar imagens preparadas pelo MCS. Sua visualização principal é dividida em quatro partes:

- Com imagem preparada sendo compartilhada entre unidades de host: No Azure e VMware



RÓTULO	PARTE	DESCRIÇÃO
A	Definições de imagem	Lista as definições de imagem criadas anteriormente.
B	Versões de imagem	Exibe as versões de imagem para a

RÓTULO	PARTE	DESCRIÇÃO
		definição de imagem selecionada. Quando **Visualizar tudo** está desativado, apenas as versões da definição de imagem selecionada são exibidas. Quando ativado, as versões de imagem de todas as definições são exibidas.
C	Detalhes	• A guia **Detalhes** exibe informações detalhadas sobre a definição ou versão de imagem selecionada, como Imagem Mestra, Recurso, Hypervisor, nome da definição de imagem, tipo de SO e tipo de sessão. • A guia **Esquema de Imagem** exibe informações sobre o modelo

RÓTULO	PARTE	DESCRIÇÃO
		usado para preparar imagens, como disco rígido, tamanho da máquina, tipo de licença, conjunto de criptografia de disco, perfil da máquina e assim por diante. • A guia **Esquemas de Provisionamento** exibe o nome do esquema de provisionamento usado para criar o catálogo. • A guia **Solução de Problemas** fornece o status de erro da versão da imagem selecionada. • No caso de compartilhamento de imagem: A guia **Recursos** fornece o status do

RÓTULO	PARTE	DESCRIÇÃO
		compartilhamento da versão da imagem.
D	Barra de ações	Lista as ações que você pode realizar em definições e versões de imagem, como **Criar Versão da Imagem**, **Editar Descrição**, **Gerenciar Compartilhamento de Imagem** (no caso de compartilhamento de imagem preparada), **Excluir Versão da Imagem** e **Criar Catálogo**.
E	Barra de pesquisa	Especifica critérios de filtro para pesquisar versões de imagem que atendam às condições.

Criar catálogos de máquinas de imagem preparada

Crie imagens preparadas e use as imagens preparadas para criar um catálogo de máquinas MCS usando:

- Studio
- Comandos PowerShell

Atualmente, você pode criar catálogos de máquinas de imagem preparada em ambientes de virtualização Amazon WorkSpaces Core Managed Instances, AWS EC2, Azure, Red Hat OpenShift, VMware e XenServer®.

> **Nota:**
>
> Você pode criar um catálogo de máquinas MCS sem usar imagens preparadas. Nesse caso, você não pode obter os benefícios do recurso. No entanto, para Amazon WorkSpaces Core Managed Instances, crie o catálogo MCS usando apenas uma versão de imagem preparada. Você não pode criar o catálogo usando uma imagem mestre diretamente.

Onde ir a seguir

- Criar catálogos usando imagens preparadas em Amazon WorkSpaces Core Managed Instances
- Criar catálogos usando imagens preparadas em AWS EC2
- Criar catálogos usando imagens preparadas em Azure
- Criar catálogos usando imagens preparadas em Red Hat OpenShift
- Criar catálogos usando imagens preparadas em VMware
- Criar catálogos usando imagens preparadas em XenServer

Criar catálogos usando imagens preparadas em instâncias gerenciadas do Amazon WorkSpaces Core

Crie imagens preparadas e use as imagens preparadas para criar um catálogo de máquinas MCS usando:

- Studio
- PowerShell

Etapas principais

1. Crie a definição da imagem e a versão inicial da imagem.
2. Crie versões de imagem a partir da versão inicial da imagem.
3. Use a versão da imagem como uma imagem preparada para criar um catálogo.

Crie uma definição de imagem e a versão inicial da imagem usando o Studio

Para criar uma definição de imagem e a versão inicial da imagem, faça o seguinte:

1. No Studio, vá para o nó **Imagens** e clique em **Criar Definição de Imagem**. Clique em **Avançar** na página **Introdução**.

2. Na página **Definição de Imagem**, especifique o **tipo de SO** e o **tipo de sessão** para a definição de imagem.
3. Na página **Imagem**, selecione **Recursos** (somente os recursos aplicáveis para a conexão definida são listados), uma imagem mestre para usar como modelo para criar a versão da imagem e um perfil de máquina para capturar propriedades de hardware. Selecione um perfil de máquina para capturar propriedades de hardware de uma instância de VM ou versão de modelo de inicialização.

> **Nota:**
>
> - Antes de selecionar uma imagem, verifique se a imagem mestre tem o VDA 2311 ou posterior instalado e se o driver MCSIO está instalado no VDA.
> - O Serviço de Metadados de Instância (IMDS) V2 é o único suportado, e não o IMDS V1. Para obter informações, consulte Como funciona o Serviço de Metadados de Instância Versão 2.

4. Na página **Especificação da Máquina**, selecione um tamanho de máquina. O tamanho da máquina do perfil da máquina (selecionado na página **Imagem**) é selecionado por padrão.
5. Na página **NICs**, selecione ou adicione NICs para a imagem de preparação. Para cada NIC, selecione uma sub-rede VPC associada.
6. Na página **Descrição da Versão**, insira uma descrição para a versão inicial da imagem criada.
7. Na página **Resumo**, verifique os detalhes da definição da imagem e da versão inicial da imagem criada. Insira um nome e uma descrição para a definição da imagem. Clique em **Concluir**.

Criar versões de imagem usando o Studio

As versões de imagem permitem o gerenciamento de diferentes iterações ou atualizações de uma imagem específica. Essa funcionalidade permite manter várias versões de uma imagem para diferentes finalidades.

Para criar versões de imagem a partir da versão inicial da imagem, faça o seguinte:

> **Nota:**
>
> A unidade de hospedagem de todas as versões de imagem deve ser a mesma.

1. Vá para o nó **Imagens**, selecione uma versão de imagem ou uma definição de imagem e clique em **Criar Versão da Imagem**.
2. Na página **Definição da imagem**, você pode alterar a unidade de hospedagem e selecionar novamente a imagem mestre e o perfil da máquina para essa versão da imagem.
3. Se você quiser que a configuração da versão da imagem seja diferente da versão inicial da imagem configurada, configure as definições nas páginas **Especificação da Máquina** e **NICs** da caixa de diálogo **Criar Versão da Imagem**.
4. Adicione uma descrição para a versão da imagem. Clique em **Concluir**.

> **Nota:**
>
> Se a criação da versão da imagem falhar por qualquer motivo, a guia **Solução de problemas** na parte inferior oferece uma opção de **Tentar novamente**.

Criar uma especificação de versão de imagem preparada usando PowerShell

Os comandos detalhados do PowerShell para criar uma especificação de versão de imagem preparada são os seguintes:

1. Verifique os nomes de definição de imagem disponíveis usando o `Test-ProvImageDefinitionNameAvailable command`. Por exemplo,

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. Crie uma definição de imagem usando o comando `New-ProvImageDefinition`. Por exemplo,

   ```
   New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
   -VdaSessionSupport MultiSession
   ```

3. Crie uma nova configuração para a definição de imagem na conexão de hospedagem especificada usando o comando `Add-ProvImageDefinitionConnection`.

   ```
   Add-ProvImageDefinitionConnection -ImageDefinitionName image1
   -HypervisorConnectionName test-conn
   ```

4. Crie uma versão de imagem usando o comando `New-ProvImageVersion`. Por exemplo,

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. Adicione uma especificação de versão de imagem mestre à versão da imagem usando o comando `Add-ProvImageVersionSpec`. Por exemplo,

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName wsc -MasterImagePath "XDHyp:
\HostingUnits\wsc\win10-2411-ami (ami-00123456789abcdef).template”"
```

> **Nota:**
>
> Você pode adicionar apenas uma especificação de versão de imagem mestre a uma versão de imagem para uma unidade de hospedagem.

6. Crie uma especificação de versão de imagem preparada a partir da especificação de versão de imagem mestre usando o comando `New-ProvImageVersionSpec`. O parâmetro `SourceImageVersionSpecUid` é derivado do comando `Add-ProvImageVersionSpec`. Por exemplo,

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  00000000-0000-0000-0000-00000000000

-MachineProfile 'XDHyp:\HostingUnits\wsc\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -RunAsynchronously
```

Exemplo do conjunto completo de comandos PowerShell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName wsc -CustomProperties $CustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\wsc\win10-2411-ami
(ami-00123456789abcdef).template”



New-ProvImageVersionSpec -MachineProfile 'XDHyp:
\HostingUnits\wsc\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
00000000-0000-0000-0000-00000000000-HostingUnitName wsc

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

Nota:

- Todas as especificações de versão de imagem em uma definição de imagem devem pertencer à mesma unidade de hospedagem.

- Uma versão de imagem pode ter apenas uma especificação de versão de imagem mestre e uma especificação de versão de imagem preparada.
- Todas as especificações de versão de imagem devem ter um perfil de máquina.

Compartilhar imagens preparadas entre zonas de disponibilidade e regiões

Agora você pode compartilhar uma única imagem preparada entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região AWS ou em regiões diferentes para suas instâncias gerenciadas do Amazon WorkSpaces Core. Isso permite que você use uma imagem preparada para criar e atualizar catálogos de máquinas MCS em várias zonas de disponibilidade e regiões. Ao compartilhar entre diferentes AZs em regiões diferentes, a versão da imagem preparada será copiada da região original para as regiões de destino.

Você pode manter uma única imagem preparada e usá-la para criar e atualizar catálogos de máquinas em várias zonas de disponibilidade e regiões vinculadas a diferentes unidades de hospedagem. Isso reduz significativamente a sobrecarga de gerenciamento de imagens, garante a consistência entre as implantações e simplifica o processo de provisionamento. Você também pode atualizar facilmente os catálogos de máquinas existentes com imagens preparadas de uma zona de disponibilidade ou região diferente.

Casos de uso

- **Gerenciamento Centralizado de Imagens:** Você cria uma imagem preparada em uma zona de disponibilidade (por exemplo, `us-east-1a`). Em seguida, você pode compartilhar essa imagem com outras zonas de disponibilidade, como `us-east-1b`, dentro da mesma região AWS `us-east-1` ou `us-west-1a` em uma `us-west-1 region` diferente. Isso permite que uma única imagem atenda a várias unidades de hospedagem e simplifica a manutenção para você.
- **Criação e Atualização Eficientes de Catálogos:** Você pode usar uma imagem preparada criada em `AZ 1` (por exemplo, `us-east-1a`) para criar novos catálogos em `AZ 1`. Depois de compartilhar esta imagem com `AZ 2` (por exemplo, `us-east-1b`), você pode usar a imagem compartilhada em `AZ 2` para criar e atualizar catálogos em `AZ 2`.
- **Implantações de unidades de hospedagem e conexões de hospedagem cruzadas:** Se seu ambiente tiver várias unidades de hospedagem na mesma ou em diferentes regiões AWS, você poderá compartilhar imagens preparadas de forma eficiente entre essas unidades de hospedagem.

Limitações

- **Compartilhamento dentro da mesma conta AWS**: Você não pode compartilhar entre diferentes contas AWS na implementação atual.

Considerações importantes

- **Ordem de exclusão:** Para excluir uma especificação de versão de imagem preparada original, você deve primeiro excluir todas as suas especificações de versão de imagem compartilhadas. Alternativamente, você deve excluir as especificações original e compartilhada simultaneamente.
- **Dependência da Versão da Imagem:** Ao remover uma versão da imagem, você deve primeiro remover quaisquer configurações de compartilhamento que dependam dessa versão específica da imagem. Os catálogos que você criou a partir da imagem original (não compartilhada) podem permanecer intactos.
- **Retrocompatibilidade do Catálogo:** Você pode atualizar catálogos de máquinas existentes que você implantou antes da introdução deste recurso. Use imagens preparadas que você criou em uma zona de disponibilidade ou região diferente daquela onde você implantou originalmente o catálogo.
- **Exclusão completa:** Ao excluir uma imagem preparada, você não poderá mais usá-la em nenhuma zona de disponibilidade onde a compartilhou ou a criou originalmente. Além disso, uma versão de imagem preparada não pode ser excluída até que todos os catálogos vinculados à versão da imagem preparada sejam excluídos primeiro.

Pré-requisitos

Antes de configurar ou usar este recurso, certifique-se de que você atende às seguintes condições:

- Seu ambiente deve ser um ambiente de Instâncias Gerenciadas do Amazon WorkSpaces Core.
- Você deve configurar várias unidades de hospedagem (cada uma pode ser vinculada a diferentes zonas de disponibilidade) e conexões de host (cada uma pode ser vinculada a uma região diferente) na mesma conta AWS.

Configurar usando a interface do usuário do Studio

Você pode compartilhar imagens preparadas entre zonas de disponibilidade vinculadas a diferentes unidades de hospedagem usando a interface do usuário do Studio.

PARA COMPARTILHAR UMA IMAGEM PREPARADA

1. navegar até o nó **Imagens** do Studio e selecione a versão da imagem preparada que você deseja compartilhar com outras zonas de disponibilidade.
2. Selecione **Gerenciar Compartilhamento de Imagem** na barra de navegação superior para gerenciar o compartilhamento de imagem para a versão de imagem selecionada.
3. Na página **Gerenciar Compartilhamento de Imagem**, selecione um ou mais recursos com os quais você deseja compartilhar a versão da imagem. Os recursos podem estar em zonas de disponibilidade diferentes da versão da imagem original.
4. Clique em **Salvar** para compartilhar a versão da imagem nos recursos em outras zonas de disponibilidade. A versão da imagem é atualizada para que seja compartilhada entre os diferentes recursos que você selecionou. Uma vez concluído, use a versão da imagem para criar catálogos nas zonas de disponibilidade em que a versão da imagem é compartilhada.

PARA REMOVER O COMPARTILHAMENTO DE UMA IMAGEM PREPARADA

1. No nó **Imagens** do Studio, selecione a versão da imagem preparada que você gostaria de remover do compartilhamento.
2. Selecione **Gerenciar Compartilhamento de Imagem** na barra de navegação superior para gerenciar o compartilhamento de imagem para a versão de imagem selecionada.
3. Desmarque as caixas de seleção de um ou mais recursos (zonas de disponibilidade) com os quais você deseja parar de compartilhar a versão da imagem.

   > **Nota:**
   >
   > Os recursos não devem mais ter nenhum catálogo associado e criado a partir da versão da imagem compartilhada. Quaisquer catálogos criados a partir da versão da imagem compartilhada a serem removidos devem ser excluídos primeiro.

4. Clique em **Salvar** para remover o compartilhamento dos recursos nas zonas de disponibilidade limpas. A versão da imagem é atualizada de forma que não seja mais compartilhada nessas zonas de disponibilidade.

Configurar usando PowerShell

Alternativamente, você pode compartilhar imagens preparadas entre zonas de disponibilidade vinculadas a diferentes unidades de hospedagem usando comandos PowerShell.

PARA COMPARTILHAR UMA IMAGEM PREPARADA

1. Certifique-se de ter o `ImageVersionSpecUid` da imagem preparada que deseja compartilhar. Você pode recuperá-lo usando `Get-ProvImageVersionSpec` ou comandos `Get-` semelhantes no PowerShell.
2. Determine o `HostingUnitName` da zona de disponibilidade (pode ser a mesma ou uma região diferente) onde você deseja disponibilizar a imagem preparada. Este é o nome da unidade de hospedagem que você configurou para essa AZ específica.
3. **Execute o comando `Add-ProvImageVersionSpecHostingUnit`:** Use o seguinte comando PowerShell. Substitua `<ImageVersionSpecUid>` pelo Uid da sua imagem e `<targetHostingUnitName>` pelo nome da unidade de hospedagem na zona de disponibilidade de destino para a qual você deseja compartilhar a especificação da versão da imagem:

   ```
   Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
   <ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
   ```

4. Após a execução bem-sucedida, você pode ver o status da imagem na interface do usuário do Studio indicando que você a compartilhou com a unidade de hospedagem especificada.

PARA REMOVER O COMPARTILHAMENTO DE UMA IMAGEM PREPARADA

1. Certifique-se de ter o `ImageVersionSpecUid` da imagem preparada da qual você deseja remover o compartilhamento.
2. Determine o `HostingUnitName` da zona de disponibilidade da qual você deseja remover a imagem compartilhada.
3. **Execute o comando `Remove-ProvImageVersionSpecHostingUnit`:** Use o seguinte comando PowerShell. Substitua `<ImageVersionSpecUid>` pelo Uid da sua imagem e `<targetHostingUnitName>` pelo nome da unidade de hospedagem na Zona de Disponibilidade de destino da qual você deseja remover o compartilhamento da especificação da versão da imagem:

   ```
   Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
   <ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
   ```

Configuração de rede durante a preparação da imagem

Durante a preparação da imagem, uma máquina virtual (VM) de preparação é criada com base na VM original. Esta VM de preparação é desconectada da rede. Para desconectar a rede da VM de

preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e saída. Este grupo de segurança de rede persiste e é reutilizado. O nome do grupo de segurança de rede é `Citrix.XenDesktop.IsolationGroup-GUID`, onde GUID é gerado aleatoriamente.

Um catálogo de máquinas baseado em perfil de máquina

Você pode usar um perfil de máquina para capturar as propriedades de hardware de uma instância EC2 (VM) ou versão de modelo de inicialização e aplicá-las às máquinas provisionadas. As propriedades capturadas podem incluir, por exemplo, tipo de locação, tipo de instância, grupos de segurança, mapeamentos de rede, propriedades de volume EBS, otimização EBS, opções de CPU, capacidade de hibernação e outras configurações AWS suportadas.

Você pode usar uma instância AWS EC2 (VM) ou uma versão de modelo de inicialização AWS como entrada do perfil de máquina.

> **Nota:**

> - As propriedades do volume EBS são derivadas apenas de um perfil de máquina.
> - O Serviço de Metadados de Instância (IMDS) V2 é o único suportado, e não o IMDS V1. Para obter informações, consulte Como funciona o Serviço de Metadados de Instância Versão 2.

Locação AWS

A AWS oferece as seguintes opções de locação: locação compartilhada (o tipo padrão) e locação dedicada. Locação compartilhada significa que várias instâncias do Amazon WorkSpaces Core de diferentes clientes podem residir na mesma peça de hardware físico. Locação dedicada significa que suas instâncias do Amazon WorkSpaces Core são executadas apenas em hardware com outras instâncias que você implantou.

> **Nota:**

> As instâncias dedicadas são as únicas suportadas (hosts dedicados não são suportados atualmente). Outros clientes não usam a mesma peça de hardware.

O tipo de locação é capturado do perfil da máquina

Ao usar o MCS para criar um catálogo para provisionar máquinas na AWS, o tipo de locação é capturado do perfil da máquina.

- **Hardware compartilhado**: Esta configuração é adequada para a maioria das implantações. Vários clientes compartilham peças de hardware, mesmo que não interajam entre si. Usar hardware compartilhado é a opção menos dispendiosa para executar suas instâncias Amazon EC2.
- **Instância dedicada**: Esta configuração é mais adequada para implantações com requisitos específicos de segurança ou conformidade. Com uma instância dedicada, você ainda desfruta dos benefícios de ter um host separado de outros clientes AWS, mas não paga pelo host inteiro. Você não precisa se preocupar com a capacidade do host, mas é cobrado a uma taxa mais alta pelas instâncias. Além disso, as Instâncias Dedicadas fornecem suporte limitado para Bring Your Own License (BYOL).

Faturamento flexível

O Amazon WorkSpaces Core Managed Instances oferece suporte a dois modos de faturamento:

MODO DE FATURAMENTO	DESCRIÇÃO
Mensal	Faturamento fixo, com taxa mensal. Ideal para desktops persistentes e cargas de trabalho previsíveis.
Por hora	Faturamento pré-pago (pay-as-you-go). Esta é a configuração padrão da AWS se nenhum modo de faturamento for explicitamente especificado.

Essas opções oferecem flexibilidade para gerenciar os custos de computação com base na persistência e nos padrões de uso da sua carga de trabalho.

Este recurso requer o uso do serviço de faturamento do Amazon WorkSpaces. Por padrão, o MCS usa este serviço para provisionar e gerenciar instâncias, permitindo que você se beneficie de preços de taxa fixa mais competitivos para cargas de trabalho persistentes.

Pré-requisitos e considerações

- Configuração da conta AWS: Sua conta AWS deve ser configurada para usar o serviço de faturamento do WorkSpaces. Embora as contas AWS sejam alternadas por padrão, alguns

clientes podem solicitar que a AWS permaneça no serviço de faturamento EC2 legado para usar o WorkSpaces Core Managed Instances.

> **Nota:**
>
> Se sua conta estiver no serviço de faturamento EC2 legado, a opção de faturamento **Mensal** não estará disponível.

- Conexão do host: O faturamento flexível é aplicável apenas a conexões de host do Amazon WorkSpaces Core. Não é compatível com conexões de host AWS EC2 padrão.
- Instâncias spot: Instâncias spot não são suportadas com o serviço de faturamento do WorkSpaces.
- Faturamento misto: Uma conta AWS deve usar o faturamento do WorkSpaces ou o faturamento do EC2 para instâncias gerenciadas principais. Uma mistura de ambos em uma única conta não é suportada.
- Compatibilidade: Apenas tipos de instância específicos, tipos de plataforma (SO) e tipos de locação são compatíveis com certos modos de faturamento. O MCS realiza uma verificação pré-voo para garantir que suas seleções (Oferta de Serviço, Perfil de Máquina e Imagem Preparada) correspondam ao modo de faturamento escolhido.

Consulte Criar um catálogo de máquinas com um modo de faturamento específico.

Criar um catálogo

Uma imagem preparada e um perfil de máquina são necessários para criar catálogos de instâncias gerenciadas do Amazon WorkSpaces Core. Você pode usar uma instância de VM AWS ou uma versão de modelo de inicialização AWS como entrada do perfil da máquina.

> **Nota:**
>
> Atualmente, a criação de catálogos de VMs persistentes e não persistentes (a propriedade `CleanOnBoot` é `True` ou `False`) é suportada.

> Antes de criar um catálogo de instâncias gerenciadas do Amazon WorkSpaces Core, você precisa concluir a criação de:

1. Uma conexão com instâncias gerenciadas do Amazon WorkSpaces Core. Consulte Conexão com instâncias gerenciadas do Amazon WorkSpaces Core
2. Uma imagem preparada.

Você pode criar um catálogo usando:

- Studio
- PowerShell

Criar um catálogo usando o Studio

Criar um catálogo de máquinas a partir do nó Imagens

Use a opção **Criar catálogo** no nó **Imagens** para criar um catálogo usando a versão da imagem.

Alternativamente, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de Máquinas**, vinculando à opção de imagem preparada no fluxo de trabalho de criação de catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas.

Para criar um catálogo de máquinas MCS a partir do nó **Imagens**, faça o seguinte:

1. Selecione uma versão da imagem e clique em **Criar catálogo**. Clique em **Avançar** na página **Introdução**.
2. Nas páginas **Gerenciamento de Máquinas** e **Imagem**, as configurações são pré-selecionadas com base na versão da imagem selecionada. Na página Imagem, insira uma nota para a imagem preparada selecionada.
3. Conclua as configurações nas páginas seguintes.
4. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.
5. Vá para o nó **Catálogos de Máquinas** para ver o catálogo de máquinas criado.

Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó Catálogos de Máquinas, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo.
2. Clique em **Criar Catálogo de Máquinas**. A página **Configuração do Catálogo de Máquinas** é exibida.
3. Na página **Tipo de Máquina**, selecione um tipo de máquina para o catálogo, por exemplo, **SO multissessão**.

4. Na página **Gerenciamento de Máquinas**, selecione as seguintes configurações:

    a. Selecione **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade)**.

    b. Selecione **Tecnologia de provisionamento Citrix**. Em seguida, selecione **Citrix Machine Creation Services™**.

    c. No campo **Recursos**, selecione os recursos (Zona de Disponibilidade ou Zona Local) que você configurou ao criar a conexão de host e clique em **Avançar**.

5. Na página **Experiência da área de trabalho**, selecione uma área de trabalho aleatória ou estática que você deseja que os usuários tenham ao fazer login. Se uma área de trabalho estática for selecionada, especifique ainda se você deseja salvar as alterações que o usuário faz no disco local (persistente ou não persistente).

6. Na página **Imagem**, clique em **Selecionar uma imagem** para selecionar uma imagem preparada para o catálogo de máquinas. Selecione a versão preparada que você criou. Clique no nome da versão da imagem. Para ver mais detalhes sobre a versão da imagem selecionada, clique no número da versão, que está sublinhado. Clique em **Concluído**.

    O perfil da máquina associado à imagem preparada aparece e suas propriedades de hardware (por exemplo, tipo de instância, tipo de locação, mapeamentos de rede, grupos de segurança, propriedades de volume) são usadas para criar máquinas nos catálogos. Para alterar a origem do perfil da máquina para outra VM ou versão de modelo de inicialização, clique no botão de edição.

7. Na página **Máquinas Virtuais**:

    a. Insira o número de VMs para o catálogo.

    b. A especificação padrão da máquina é exibida, que é baseada no perfil da máquina. Para alterá-la, selecione o ícone de edição e selecione uma especificação de máquina.

8. Na página **NICs**, selecione as NICs (ou ENIs) para as VMs.

9. Na página **Identidades da Máquina**, configure o tipo de identidade da máquina para as máquinas no catálogo:

    a. Para configurar **máquinas ingressadas no domínio (Active Directory local ou Microsoft Entra híbrido)**, selecione o domínio e crie novas contas AD para as VMs a serem criadas neste catálogo de máquinas. As VMs provisionadas são ingressadas no domínio selecionado. Para provisionar **máquinas não ingressadas no domínio**, selecione a opção de não ingresso no domínio.

b. Especifique o esquema de nomenclatura de conta para as novas contas a serem criadas para as VMs.

10. Na página **Credenciais de domínio**, clique em **Inserir credenciais** para fornecer as credenciais para o domínio selecionado. Insira o nome de usuário e a senha de nível de administrador quando solicitado. Você também pode usar uma conta de serviço se já tiver credenciais de domínio salvas anteriormente, seguindo nossa documentação do produto.
11. Clique nas páginas restantes até a página **Resumo**. Insira um nome para o catálogo de máquinas e selecione **Concluir** para criar o catálogo de máquinas.

Limitações na criação de um catálogo de máquinas em uma zona local da AWS

- Certas zonas locais suportam apenas determinadas configurações de hardware (por exemplo, a zona local de Perth não suporta volumes GP3, apenas GP2).
- Como apenas gp2 é universalmente suportado em todas as zonas locais, e nem todas suportam gp3, a criação de disco de ID padroniza o uso do tipo de volume gp2.
- Você deve selecionar um perfil de máquina com especificações de hardware que sejam suportadas na zona local desejada.
- Os snapshots de AMIs de imagem preparada e os snapshots de disco de ID são padronizados para serem colocados na região, em vez da zona local (devido a limitações da AWS em relação à visibilidade do suporte a snapshots EBS em zonas locais).
- Apenas zonas locais que suportam serviços completos de EC2 e EBS são zonas suportadas.

Criar um catálogo usando PowerShell

Criar um catálogo usando uma especificação de versão de imagem preparada e perfil de máquina

- Crie um catálogo de máquinas não persistentes do MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$true] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

- Crie um catálogo de máquinas persistentes do MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$false] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

Exemplo do conjunto completo de comandos Powershell para criar um catálogo:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "wsccatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "domainname"
-IdentityPoolName "wsccatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "aws##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName wsccatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName wsc -IdentityPoolName wsccatalog -CleanOnBoot -Scope @()
-SecurityGroup @() -MachineProfile 'XdHyp:\HostingUnits\cvad-test-
scalestress\us-east-1a.availabilityzone\machine-profile-instance i
(i-0xxxxxxx).vm' -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName wsccatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Atualizar o perfil da máquina

Para atualizar o perfil da máquina em um catálogo que foi inicialmente provisionado com um perfil de máquina, faça o seguinte. Você também pode alterar o tipo de locação e a capacidade de hibernação da origem do perfil da máquina ao editar um catálogo de máquinas MCS.

1. Execute o comando `Set-ProvScheme`. Por exemplo,

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

Criar um catálogo de máquinas com um modo de faturamento específico

Você pode especificar o modo de faturamento ao criar um catálogo de máquinas usando apenas o PowerShell atualmente.

Para especificar o modo de faturamento através do PowerShell, use o parâmetro `CustomProperties` no comando `New-ProvScheme`.

```
$custprop = "BillingMode,Monthly"



New-ProvScheme -ProvisioningSchemeName "MyCatalog" `

-ImageVersionSpecUid $ImageVersionSpecUid `

-HostingUnitName "wsc-unit" `

-IdentityPoolName "MyIdentityPool" `

-MachineProfile "XdHyp:\HostingUnits\wsc-unit\machine-profile
lt-123.launchtemplate\lt-123 (1).launchtemplateversion" `

-CustomProperties $custprop `

-CleanOnBoot
```

> **Nota:**
>
> Se a propriedade `BillingMode` for omitida, o catálogo assume o padrão `Hourly`.

ALTERAR O MODO DE FATURAMENTO DE UM CATÁLOGO EXISTENTE

Você pode converter um catálogo existente de `Monthly` para `Hourly`, ou vice-versa. Essa alteração pode ser aplicada a VMs novas e existentes no catálogo.

CONSIDERAÇÕES IMPORTANTES PARA ATUALIZAÇÕES

- Janela de serviço: As VMs existentes devem passar por uma janela de serviço ou ciclo de energia para aplicar a alteração de faturamento.
- Validação: O MCS valida se os tipos de instância e plataformas existentes são compatíveis com o novo modo de faturamento antes de aplicar a alteração.

ATUALIZAR USANDO O POWERSHELL

- Para atualizar o modo de faturamento apenas de novas VMs adicionadas a um catálogo, atualize a propriedade personalizada do modo de faturamento do esquema de provisionamento:

```
$custprop = "BillingMode,Hourly"



Set-ProvScheme -ProvisioningSchemeName "MyCatalog" -CustomProperties
$custprop
```

- Para atualizar o modo de faturamento de VMs novas e existentes em um catálogo, crie uma nova versão do esquema de provisionamento com a propriedade personalizada atualizada e aplique a nova versão a todas as VMs:

```
$custprop = "BillingMode,Hourly"



New-ProvSchemeVersion -ProvisioningSchemeName "MyCatalog"
-CustomProperties $custprop
```

```
New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 2 `
-StartsNow -AllVMs `
-MaxDurationInMinutes 100 `
-ProvisioningSchemeName "MyCatalog"
```

MONITORAR INFORMAÇÕES DE FATURAMENTO

Você pode verificar o modo de faturamento para catálogos e máquinas virtuais individuais.

Execute os seguintes comandos do PowerShell para verificar a elegibilidade de faturamento da sua conta:

- Retorna `BillingMode` como parte de CustomProperties

```
Get-ProvScheme –ProvisioningSchemeName “"MyCatalog" "  | Select
 ProvisioningSchemeName,  CustomProperties
```

- Retorna `BillingMode` como parte de VMInfo

```
Get-ProvVMDetails –ProvisioningSchemeName “"MyCatalog" "  | Select-
Object  -ExpandProperty VMInfo
```

SOLUÇÃO DE PROBLEMAS E VALIDAÇÃO

O MCS inclui verificações de pré-voo para evitar configurações incompatíveis. Você pode encontrar os seguintes erros durante a criação ou edição do catálogo:

- **NoInstanceConfigFoundForBillingMode**: Ocorre se a Oferta de Serviço (tipo de instância), Tenancy e Tipo de Plataforma selecionados não forem suportados para o modo de faturamento escolhido.
- **Spot Instance Not Supported**: Se você tentar usar instâncias Spot com uma conexão de host do WorkSpaces, a validação falhará.
- **Restrição de faturamento do EC2**: Se sua conta AWS estiver no modelo de faturamento legado do EC2, tentar definir um modo de faturamento Mensal resultará em um erro de validação.

Criar um catálogo com versão de modelo de inicialização usando PowerShell

Você pode criar um catálogo de máquinas MCS com uma versão de modelo de inicialização como entrada de perfil de máquina. Você também pode atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização e de uma versão de modelo de inicialização para uma VM.

No console AWS EC2, você pode fornecer as informações de configuração da instância de um modelo de inicialização junto com o número da versão. Ao especificar a versão do modelo de inicialização como entrada de perfil de máquina durante a criação ou atualização de um catálogo de máquinas, as propriedades dessa versão do modelo de inicialização são copiadas para as VMs VDA provisionadas.

As seguintes propriedades podem ser fornecidas usando a entrada do perfil da máquina ou explicitamente como parâmetros nos comandos `New-ProvScheme` ou `Set-ProvScheme`. Se forem fornecidas nos comandos `New-ProvScheme` ou `Set-ProvScheme`, elas terão precedência sobre os valores do perfil da máquina dessas propriedades.

- Oferta de Serviço
- Redes

> **Nota:**
>
> Se a oferta de serviço não for fornecida no modelo de inicialização do perfil da máquina ou como um parâmetro no comando `New-ProvScheme`, você receberá um erro apropriado.

> Para criar um catálogo usando a versão do modelo de inicialização como entrada de perfil de máquina:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Obtenha a lista de versões de modelo de inicialização de um modelo de inicialização. Por exemplo:

   ```
   XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
   Select FullPath
   ```

4. Crie um pool de identidades, se ainda não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. Crie um esquema de provisionamento com uma versão de modelo de inicialização como entrada de perfil de máquina. Por exemplo:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-ImageVersionSpecUid ‘24dfb047-e867-527g-896c-25664xxxxx1t’ `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. Registre um esquema de provisionamento como um catálogo de broker. Por exemplo:

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `
```

```
-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. Conclua a criação do catálogo.

Atualizar a origem do perfil de máquina

Você também pode atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização e de uma versão de modelo de inicialização para uma VM. Por exemplo:

- Para atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- Para atualizar a entrada de um catálogo de perfil de máquina de uma versão de modelo de inicialização para uma VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

Catálogo habilitado para MCSIO

A Otimização de Armazenamento MCS (MCSIO) melhora o desempenho de E/S da máquina virtual armazenando em cache as operações de gravação em disco por meio de um mecanismo de duas camadas:

- na memória, ou
- em um disco dedicado de alta velocidade (transborda para o disco quando a memória está cheia).

Para instâncias gerenciadas do Amazon WorkSpaces Core, habilitar o MCSIO anexa um disco de Cache de Gravação (WBC) a cada VM provisionada, além dos discos padrão de SO e Identidade.

Habilite e configure o MCSIO usando:

- Studio
- PowerShell

Use o Studio para habilitar o MCSIO

PRÉ-REQUISITOS

Antes de configurar o MCSIO no Studio, certifique-se do seguinte:

- O driver MCSIO está instalado na imagem mestre (AMI). Ao instalar ou atualizar o VDA, selecione a opção para instalar o driver MCSIO. Por padrão, o driver não é instalado.
- Uma versão de imagem preparada é criada a partir de uma imagem mestre que inclui o driver MCSIO.
- O catálogo de máquinas usa uma experiência de desktop não persistente (CleanOnBoot). O MCSIO se aplica a catálogos VDI não persistentes.

CRIE UM CATÁLOGO DE MÁQUINAS HABILITADO PARA MCSIO USANDO O STUDIO

Conclua as etapas anteriores de criação de catálogo (Tipo de Máquina, Gerenciamento de Máquina, Experiência de Desktop, Imagem, Máquinas Virtuais, NICs, Identidades de Máquina, Credenciais de Domínio) conforme descrito em Criar um catálogo. Ao chegar à página Configurações de Disco, faça o seguinte:

1. Na página **Configurações de Disco**, selecione a caixa de seleção **Habilitar e configurar cache de gravação para desempenho ideal de E/S**.
2. Configure as configurações do disco de cache de gravação:
    - **Tamanho do cache de disco (GB)**: Insira o tamanho em gigabytes do disco usado para cache. O valor deve ser de pelo menos 1 GB e não deve exceder o tamanho do disco do SO.
    - **Letra da unidade de disco**: Selecione Atribuição automática para permitir que o sistema atribua uma letra de unidade, ou especifique uma letra de unidade manualmente.
    - **Memória alocada para cache (MB)**: Insira a quantidade de memória em megabytes a ser alocada para cache. O valor deve ser maior que zero e menor que a memória total da máquina.

> **Nota:**
>
> O cache de write-back exige que o driver MCSIO esteja instalado na imagem mestre.

3. Em **Selecionar o tipo de armazenamento para o disco de cache de write-back**, selecione um tipo de volume EBS SSD:

   Tipo de Armazenamento:

   - SSD de Uso Geral (gp2)
   - SSD de Uso Geral (gp3)
   - SSD de IOPS Provisionadas (io1)
   - SSD de IOPS Provisionadas (io2)

   > **Nota:**
   >
   > O cache de write-back suporta apenas tipos de volume EBS SSD. Tipos de volume HDD e armazenamento de instância local (armazenamento efêmero) não são suportados.

4. Em **Selecionar o tipo de persistência para o disco de cache de write-back**, selecione uma das seguintes opções:

   - **Usar disco de cache de write-back não persistente**: O disco de cache é criado quando a máquina é ligada e excluído quando é desligada. Este é o padrão.
   - **Usar disco de cache de write-back persistente**: O disco de cache é retido entre os ciclos de energia.

5. Em **Disco do sistema**, opcionalmente, selecione **Reter disco do sistema durante ciclos de energia** para manter o disco do SO quando a máquina for desligada. Quando ativado, as máquinas pulam a recriação do disco raiz a partir do modelo em cada inicialização, o que reduz o tempo de inicialização.

   > **Nota:**
   >
   > Para um desempenho de inicialização ideal, ative **Usar disco de cache de write-back persistente** e **Reter disco do sistema durante ciclos de energia**. Com ambas as

> opções ativadas, as máquinas reutilizam o disco de cache e o disco do SO existentes na inicialização, em vez de inicializar novos.

6. Clique em **Avançar** para prosseguir pelas páginas restantes do assistente.
7. Na página **Resumo**, verifique as configurações relacionadas ao MCSIO antes de finalizar. O resumo exibe os seguintes campos de cache de write-back:
   - Ativar cache de disco temporário
   - Tamanho do cache de memória (MB)
   - Tamanho do cache de disco (GB)
   - Persistente com disco de cache de write-back
   - Tipo de disco de cache de write-back
   - Letra da unidade do disco de cache de write-back
   - Reter disco do sistema
8. Insira um nome e uma descrição opcional para o catálogo de máquinas e clique em **Concluir**.

ATUALIZAR CONFIGURAÇÕES DO MCSIO EM UM CATÁLOGO EXISTENTE USANDO O STUDIO

Você pode atualizar as configurações de cache de write-back em um catálogo existente em **Editar Catálogo de Máquinas**.

> **Nota:**
>
> As alterações feitas na página **Configurações de Disco** aplicam-se apenas a novas máquinas que você adicionar ao catálogo posteriormente. As máquinas existentes permanecem inalteradas.

1. Em **Catálogos de Máquinas**, selecione o catálogo a ser atualizado e clique em **Editar Catálogo de Máquinas**.
2. navegar para a página **Configurações de Disco**. Atualize qualquer uma das seguintes configurações:
   - **Tamanho do cache de disco (GB)**: Altere o tamanho do disco de cache de write-back.
   - **Memória alocada para cache (MB)**: Altere a memória alocada para o cache.

- **Tipo de armazenamento**: Altere o tipo de volume EBS para o disco de cache de write-back.
- **Tipo de persistência**: Alterne entre disco de cache de write-back persistente e não persistente.
- **Reter disco do sistema durante ciclos de energia**: Habilite ou desabilite a retenção do disco do SO.

3. Clique em **Aplicar** para salvar sem fechar, ou em **Salvar** para salvar e fechar.

LAYOUT DO DISCO EBS PARA MÁQUINAS COM MCSIO HABILITADO

Quando o MCSIO está habilitado, cada VM do Amazon WorkSpaces Core provisionada tem três volumes EBS anexados. Você pode verificar o layout do disco no AWS Management Console, na seção Elastic Block Store dos detalhes da instância EC2.

DISCO	ÍNDICE DO DISPOSITIVO	DESCRIÇÃO
Disco do SO	/dev/sda1	Volume raiz clonado da imagem preparada. Se a opção Retain system disk during power cycles estiver ativada, este disco persistirá quando a máquina for desligada.
Disco de identidade	o xvdf	Armazena informações de identidade da máquina para a VM provisionada. Sempre persiste.
Disco de cache de write-back	o xvdg	Disco de cache de alta velocidade para operações de gravação MCSIO. Persiste entre ciclos de energia somente se a opção Use persistent write-back cache disk estiver selecionada.

REFERÊNCIA DE COMPORTAMENTO DO CACHE DE WRITE-BACK E DO DISCO DO SO

A tabela a seguir resume como o cache de write-back e o disco do SO se comportam com base nas configurações de persistência selecionadas.

PERSISTÊNCIA DO WBC	RETENÇÃO DO DISCO DO SO	AO DESLIGAR	DESEMPENHO DE INICIALIZAÇÃO	CUSTOS DE ARMAZENAMENTO QUANDO A VM É DESLIGADA
Não persistente (padrão)	Desabilitado (padrão)	Tanto o disco WBC quanto o disco do SO são excluídos. Novos discos são criados na próxima inicialização.	Padrão	Sem custos de disco do SO ou disco WBC.
Não persistente (padrão)	Habilitado	O disco WBC é excluído. O disco do SO é retido.	Mais rápido — ignora a inicialização do disco do SO	Custos de disco do SO, sem custos de disco WBC.
Persistente	Desabilitado (padrão)	O disco WBC é retido. O disco do SO é excluído e recriado a partir do modelo na próxima inicialização.	Mais rápido — ignora a inicialização do WBC	Custos de disco WBC, sem custos de disco do SO.
Persistente	Ativado	Tanto o disco WBC quanto o disco do SO são retidos.	Mais rápido — nenhuma inicialização de disco é necessária	Custos de disco do SO e disco WBC.

Nota:

Ativar a retenção do disco do SO em um catálogo não persistente significa que o disco do SO não é redefinido na reinicialização. Isso troca tempos de inicialização mais rápidos por custos de armazenamento do disco do SO. Todas as gravações, no entanto, ainda vão apenas para o cache de memória Write-back ou disco de cache Write-back. As alterações do

usuário não são acumuladas no disco do SO mesmo ao ativar a retenção do disco do SO. Avalie com base nos requisitos do seu ambiente.

USE O POWERSHELL PARA ATIVAR O MCSIO

CRIE UM CATÁLOGO HABILITADO PARA MCSIO USANDO O POWERSHELL

Os quatro parâmetros adicionados ao comando New-ProvScheme do PowerShell são:

- `UseWriteBackCache`: Ativa o cache (cache de write-back) para o esquema de provisionamento fornecido
- `WriteBackCacheDiskSize`: Especifica o tamanho em GB do disco temporário usado para cache
- `WriteBackCacheMemorySize`: Especifica a quantidade de memória em MB a ser usada para cache. Este é um parâmetro opcional.

Nota:

- O valor de `WriteBackCacheDiskSize` deve ser maior que zero porque é necessário pelo menos 1 GB de armazenamento em disco de cache. O tamanho do disco de cache não deve ser maior que o tamanho do disco do SO.
- O valor de `WriteBackCacheMemorySize` deve ser diferente de zero e menor que o tamanho da memória do catálogo de máquinas.

As propriedades personalizadas que afetam o MCSIO são:

- `WBCDiskStorageType`: Define o tipo de volume, que é usado para o disco temporário em instâncias gerenciadas do Amazon WorkSpaces Core. Este parâmetro aceita um argumento de string no formato `volume-type[:iops][:throughput]`. Os seguintes são os tipos de volume:
  - gp2: Não use os parâmetros iops e throughput para este tipo de volume
  - gp3: Use os parâmetros iops e throughput para este tipo de volume
  - io1: Use apenas o parâmetro iops para este tipo de volume
  - io2: Use apenas o parâmetro iops para este tipo de volume

  O tipo de volume padrão é **gp2**.

- `PersistWBC`: Controla se o disco de cache deve ser mantido ou descartado sempre que as instâncias gerenciadas do Amazon WorkSpaces Core forem desligadas. Se definido como `true`, o disco de cache é mantido. Se definido como `false` (o padrão), o disco de cache é criado e mantido apenas enquanto a instância AMI estiver ligada.
- `PersistOSDisk`: Controla se o disco do SO deve ser mantido ou descartado sempre que as instâncias gerenciadas do Amazon WorkSpaces Core forem desligadas. Se definido como `true`, o disco do SO é mantido. Se definido como `false` (o padrão), o disco do SO é criado e mantido apenas enquanto a instância AMI estiver ligada.

Execute as seguintes etapas na janela do PowerShell para criar um catálogo não persistente habilitado para MCSIO:

1. Abra a janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um catálogo de broker e um pool de identidade.
4. Crie o esquema de provisionamento. Por exemplo:

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'



$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
```

```
- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. Adicione VMs ao catálogo.

Melhore o desempenho de inicialização com MCSIO

Você pode melhorar o desempenho de inicialização de VMs se habilitar o MCSIO e definir as propriedades personalizadas `PersistWBC` e `PersistOSDisk` como `true`. Com essa configuração, as VMs podem inicializar mais rapidamente porque não precisam inicializar um novo disco de cache ou recriar um disco raiz a partir de seu modelo.

Criptografar discos de SO e ID

Você pode criar um catálogo de VMs com chaves AWS KMS (chave gerenciada pelo cliente e chave gerenciada pela AWS) que podem ser usadas para criptografar o disco do SO e o disco de identidade (ID).

- As chaves gerenciadas pela AWS são rotacionadas automaticamente todos os anos.
- As chaves gerenciadas pelo cliente são opcionais para rotação automática e podem ser gerenciadas manualmente.

Você pode consultar os seguintes documentos da AWS para obter mais informações sobre chaves KMS:

- Conceitos do AWS KMS
- Como funciona a rotação automática de chaves

Para criptografia de discos de SO e ID, configure uma das seguintes opções:

- Use uma imagem preparada que esteja criptografada (por exemplo, uma AMI criada a partir de uma instância ou snapshot que contém um volume raiz EBS criptografado com chave KMS)

- Use uma fonte de perfil de máquina (VM ou modelo de inicialização) que contenha um volume raiz EBS criptografado.

Limitações

Considere as seguintes limitações:

- O MCS atualmente suporta apenas um disco na AMI de imagem preparada.
- Você não pode criptografar diretamente volumes ou snapshots EBS existentes não criptografados, nem modificar a chave KMS de um volume criptografado existente. Para fazer isso, você deve:

  a. Criar um novo snapshot desse volume.

  b. Criar um novo volume a partir desse snapshot

  c. Criptografar o novo volume.

Consulte os seguintes documentos da AWS:

- Criptografar recursos não criptografados
- Limitações da criptografia automática ou padrão de volumes EBS: Criptografar automaticamente volumes EBS existentes e novos da Amazon.

Criar um catálogo com criptografia de disco

Você pode criar um catálogo de máquinas MCS com criptografia de disco usando:

- Imagem preparada (criada usando gerenciamento de imagem a partir de uma imagem mestre que possui disco criptografado)
- Perfil de máquina

As considerações ao usar a entrada do perfil da máquina são:

- A chave KMS da entrada do perfil da máquina tem precedência sobre a chave KMS da imagem preparada.
- Se nenhuma entrada de perfil de máquina for fornecida, a chave KMS da AMI da imagem preparada será usada para criptografar os discos das VMs do catálogo.
- Se o perfil da máquina tiver Mapeamentos de Dispositivo de Bloco presentes, os dispositivos de bloco presentes no modelo de imagem preparada (AMI) e no perfil da máquina devem corresponder. Por exemplo, se a AMI tiver um dispositivo definido em `/dev/sda1`, o Perfil da Máquina também deve ter um dispositivo definido em `/dev/sda1`.

- Se não houver chave na origem do perfil da máquina e a imagem preparada não estiver criptografada, os discos das VMs do catálogo não serão criptografados.
- Quando a imagem preparada é criptografada, uma VM de origem do perfil da máquina ou um modelo de inicialização deve ter um volume raiz criptografado para ser considerado uma entrada válida.

Modificar um catálogo existente

Você pode modificar um catálogo existente usando o comando PowerShell `Set-ProvScheme` para ter:

- Uma entrada de perfil de máquina com um volume contendo uma nova chave KMS.
- Uma imagem preparada criada a partir da imagem mestre com AMI criptografada usando gerenciamento de imagem.

Considerações importantes:

- Os volumes das novas VMs adicionadas ao catálogo são criptografados com a nova chave KMS.
- Para atualizar as configurações de criptografia quando houver um perfil de máquina existente, execute `Set-ProvScheme` com um novo perfil de máquina.
- Você não pode modificar um catálogo existente de volumes criptografados para volumes não criptografados. Você não pode fazer uma atualização de imagem de uma AMI de imagem preparada criptografada para uma AMI de imagem preparada não criptografada.

Habilitar NitroTPM e inicialização segura UEFI para instâncias de VM

Ao criar um catálogo, agora você pode selecionar uma imagem preparada (AMI) com NitroTPM e/ou inicialização segura UEFI habilitados. Consequentemente, as VMs provisionadas no catálogo também são habilitadas com NitroTPM e/ou inicialização segura UEFI. Essa implementação garante que as VMs sejam seguras e confiáveis. Para obter mais informações sobre NitroTPM e Inicialização Segura UEFI, consulte a documentação da Amazon.

Limitações

- Atualmente, você pode usar o NitroTPM e o Secure Boot em todas as regiões da AWS (incluindo as regiões AWS GovCloud (US)), exceto na China.
- Você não pode habilitar o NitroTPM e o Secure Boot UEFI em catálogos existentes. Se você deseja um catálogo com NitroTPM e Secure Boot UEFI habilitados, crie um novo catálogo.

Principais etapas

1. Configure seu ambiente AWS.
2. Crie uma conexão com a AWS.
3. Crie uma imagem mestre (AMI) habilitada com NitroTPM e/ou Secure Boot UEFI.
4. Crie uma imagem preparada a partir da imagem mestre. Consulte Criar uma imagem preparada para instâncias gerenciadas do Amazon WorkSpaces Core.
5. Crie um catálogo de máquinas selecionando a imagem preparada com NitroTPM e Secure Boot UEFI habilitados no menu de criação de catálogo do Citrix Studio ou ao criar um Esquema de Provisionamento usando comandos PowerShell.

As VMs adicionadas ao catálogo criado têm NitoTPM e Secure Boot UEFI habilitados.

Crie uma AMI que suporte NitroTPM e Secure Boot UEFI

1. Você pode criar uma AMI a partir de uma VM que tenha NitroTPM e/ou Secure Boot UEFI habilitados.
   a. Crie a instância usando as imagens do AWS Marketplace. Por exemplo, pesquise por `TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`.
   b. Baixe o VDA de sessão única ou múltipla.
   c. Crie uma AMI a partir dessa VM.
2. Use o comando register-image:

   ```
   --boot-mode (string)

   --tpm-support (string)
   ```

   Para obter mais informações, consulte register-image.

Consulte os seguintes documentos da AWS:

- Determine os modos de inicialização compatíveis de um tipo de instância EC2
- Requisitos para usar o NitroTPM com instâncias do Amazon EC2/.

Você pode abrir uma janela do PowerShell no host do Delivery Controller™ para verificar se um específico:

- oferta de serviço suporta NitroTPM ou inicialização segura UEFI

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- modelo suporta NitroTPM ou inicialização segura UEFI

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

Atualizar a oferta de serviço do catálogo existente

Você pode alterar a oferta de serviço de um catálogo existente usando `Set-ProvScheme`. A alteração se aplica às VMs recém-adicionadas. No entanto, você recebe erros nos seguintes cenários:

MODO DE INICIALIZAÇÃO DAS AMIS	A AMI SUPORTA NITRO TPM?	A OFERTA DE SERVIÇO SUPORTA NITROTPM E INICIALIZAÇÃO SEGURA UEFI?
UEFI	Não	Não
BIOS Legado	Sim	Não
UEFI	Sim	Não
UEFI Preferencial	Sim	Não

Copiar tags em VMs

Você pode copiar tags em NICs e discos (disco de identidade, disco de cache de gravação e disco do SO) que são especificados no perfil da máquina para VMs recém-criadas em um catálogo de máquinas MCS. Você pode especificar essas tags em qualquer uma das fontes de perfil da

máquina (instância de VM AWS ou versão de modelo de inicialização AWS). Este recurso é aplicável a catálogos de máquinas e VMs persistentes e não persistentes.

Nota:

- No console do AWS EC2, você não pode ver os valores de **Tag Network Interfaces** em **Launch Template Version Resource Tags**. No entanto, você pode executar o comando PowerShell `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` para ver as especificações da tag.
- Se uma fonte de perfil de máquina (VM ou versão de modelo de inicialização) tiver duas interfaces de rede (eni-1 e eni-2), e eni-1 tiver a tag t1 e eni-2 tiver a tag t2, então a VM receberá as tags de ambas as interfaces de rede.

Filtrar instâncias de VM usando PowerShell

Uma instância de VM da AWS que você usa como VM de perfil de máquina deve ser compatível para que o catálogo de máquinas seja criado e funcione corretamente. Para listar as instâncias de VM da AWS que podem ser usadas como VMs de entrada de perfil de máquina, você pode usar o comando `Get-HypInventoryItem`. O comando pode paginar e filtrar o inventário de VMs disponíveis em uma unidade de hospedagem.

Paginação:

Get-HypInventoryItem oferece suporte a dois modos de paginação:

- O modo de paginação usa os parâmetros `-MaxRecords` e `-Skip` para retornar conjuntos de itens:
  - `-MaxRecords`: O padrão é **1**. Isso controla quantos itens retornar.
  - `-Skip`: O padrão é **0**. Isso controla quantos itens ignorar desde o início absoluto (ou fim absoluto) da lista no hipervisor.
- O modo de rolagem usa os parâmetros `-MaxRecords`, `-ForwardDirection` e `-ContinuationToken` para permitir a rolagem dos registros:
  - `-ForwardDirection`: O padrão é **True**. Isso é usado junto com `-MaxRecords` para retornar o próximo conjunto de registros correspondentes ou o conjunto anterior de registros correspondentes.

- `-ContinuationToken`: Retorna os itens imediatamente depois (ou antes, se `ForwardDirection` for **false**), mas não incluindo o item fornecido em `ContinuationToken`.

Exemplos de paginação:

- Para retornar um único registro do modelo de máquina com o nome mais baixo. O campo `AdditionalData` tem o `TotalItemsCount` e o `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- Para retornar 10 registros do modelo de máquina com o nome mais baixo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- Para retornar um array de registros terminando com o nome mais alto:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- Para retornar um array de registros começando no modelo de máquina associado ao `ContinuationToken` fornecido:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

Filtragem:

Os seguintes parâmetros opcionais adicionais são suportados para filtragem. Você pode combinar esses parâmetros com as opções de paginação.

- `-ContainsName "my_name"`: Se a string fornecida corresponder a parte de um nome de AMI, a AMI será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: Se uma AMI tiver pelo menos uma dessas tags, ela será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **Nota:**
>
> Dois valores de tag são suportados. O valor da tag **Não Marcado** corresponde a itens que não possuem a tag fornecida em sua lista de tags. O valor da tag **Todos os valores** corresponde a itens que possuem a tag, independentemente do valor da tag. Caso contrário, a correspondência ocorre apenas se o item tiver a tag e o valor for igual ao que é fornecido no filtro.

- `-Id "ami-0a2d913927e0352f3"`: Se a AMI corresponder ao ID fornecido, ela será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

Filtragem no parâmetro AdditionalData:

O parâmetro de filtro `AdditionalData` lista modelos ou VMs com base em sua capacidade, oferta de serviço ou qualquer propriedade que esteja em AdditionalData. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

Você também pode adicionar um parâmetro `-Warn` para indicar as VMs incompatíveis. As VMs são incluídas com um campo `AdditionalData` chamado **Aviso**. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

Onde ir a seguir

- Gerenciar catálogos criados usando imagens preparadas

Mais informações

- Gerenciamento de imagens
- Para exemplos de PowerShell do GitHub do Amazon WorkSpaces Core, consulte citrix-mcs-sdk-samples-Amazon WorkSpaces Core

Criar catálogos usando imagens preparadas no AWS EC2

Crie imagens preparadas e use as imagens preparadas para criar um catálogo de máquinas MCS usando:

- Studio
- Comandos PowerShell

As etapas principais para criar um catálogo de máquinas MCS usando a imagem preparada são:

1. Crie a definição da imagem e as versões iniciais da imagem.
2. Use a versão da imagem como uma imagem preparada para criar um catálogo

Criar uma definição de imagem e uma versão inicial da imagem

Usar o Studio

Para criar uma definição de imagem e a versão inicial da imagem, faça o seguinte:

1. No Studio, vá para o nó **Imagens** e clique em **Criar Definição de Imagem**. Clique em **Avançar** na página **Introdução**.
2. Na página **Definição de Imagem**, especifique o **Tipo de SO** e o **Tipo de Sessão** para a definição da imagem.
3. Na página **Imagem**, selecione **Recursos** (somente os recursos aplicáveis para a conexão definida são listados), uma imagem mestre para usar como modelo para criar a versão da imagem e um perfil de máquina para capturar propriedades de hardware. Selecione um perfil

de máquina para capturar propriedades de hardware de uma instância de VM ou versão de modelo de inicialização.

> **Nota:**
>
> - Antes de selecionar uma imagem, verifique se a imagem mestre tem o VDA 2311 ou posterior instalado e se o driver MCSIO está instalado no VDA.
> - O Serviço de Metadados de Instância (IMDS) V1 e V2 são ambos suportados.

4. Na página **Especificação da Máquina**, selecione um tamanho de máquina. O tamanho da máquina do perfil da máquina (selecionado na página **Imagem**) é selecionado por padrão.
5. Na página **NICs**, selecione ou adicione NICs para a imagem de preparação. Para cada NIC, selecione uma sub-rede VPC associada.
6. Na página **Descrição da Versão**, insira uma descrição para a versão inicial da imagem criada.
7. Na página **Resumo**, verifique os detalhes da definição da imagem e da versão inicial da imagem criada. Insira um nome e uma descrição para a definição da imagem. Clique em **Concluir**.

CRIAR VERSÕES DE IMAGEM

As versões de imagem permitem o gerenciamento de diferentes iterações ou atualizações para uma imagem específica. Essa funcionalidade permite que você mantenha várias versões de uma imagem para diferentes propósitos.

Para criar versões de imagem a partir da versão inicial da imagem, faça o seguinte:

> **Nota:**
>
> A unidade de hospedagem de todas as versões da imagem deve ser a mesma.

1. Vá para o nó **Imagens**, selecione uma versão de imagem ou uma definição de imagem e clique em **Criar Versão da Imagem**.
2. Na página **Definição da imagem**, você pode alterar a unidade de hospedagem e selecionar novamente a imagem mestre e o perfil da máquina para essa versão da imagem.

3. Se você quiser que a configuração da versão da imagem seja diferente da versão inicial da imagem configurada, configure as definições nas páginas **Especificação da Máquina** e **NICs** da caixa de diálogo **Criar Versão da Imagem**.
4. Adicione uma descrição para a versão da imagem. Clique em **Concluir**.

> **Nota:**
>
> Se a criação da versão da imagem falhar por qualquer motivo, a guia **Solução de problemas** na parte inferior fornece uma opção de **Repetir**.

Usar PowerShell

Os comandos detalhados do PowerShell para criar uma especificação de versão de imagem preparada são os seguintes:

1. Verifique os nomes de definição de imagem disponíveis usando `Test-ProvImageDefinitionNameAvailable command`. Por exemplo,

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. Crie uma definição de imagem usando o comando `New-ProvImageDefinition`. Por exemplo,

   ```
   New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
   -VdaSessionSupport MultiSession
   ```

3. Crie uma nova configuração para a definição de imagem na conexão de hospedagem especificada usando o comando `Add-ProvImageDefinitionConnection`.

   ```
   Add-ProvImageDefinitionConnection -ImageDefinitionName image1
   -HypervisorConnectionName test-conn
   ```

4. Crie uma versão de imagem usando o comando `New-ProvImageVersion`. Por exemplo,

   ```
   New-ProvImageVersion -ImageDefinitionName image1 -Description "version
   1"
   ```

5. Adicione uma especificação de versão de imagem mestre à versão da imagem usando o comando `Add-ProvImageVersionSpec`. Por exemplo,

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName aws -MasterImagePath "XDHyp:
\HostingUnits\aws\win10-2411-ami (ami-00123456789abcdef).template”"
```

> **Nota:**
>
> Você pode adicionar apenas uma especificação de versão de imagem mestre a uma versão de imagem para uma unidade de hospedagem.

6. Crie uma especificação de versão de imagem preparada a partir da especificação de versão de imagem mestre usando o comando `New-ProvImageVersionSpec`. O parâmetro `SourceImageVersionSpecUid` é derivado do comando `Add-ProvImageVersionSpec`. Por exemplo,

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  00000000-0000-0000-0000-00000000000

-MachineProfile 'XDHyp:\HostingUnits\aws\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -RunAsynchronously
```

Exemplo do conjunto completo de comandos do PowerShell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession




Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName aws-CustomProperties $CustomProperties
```

```
$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\aws\win10-2411-ami
(ami-00123456789abcdef).template”



New-ProvImageVersionSpec -MachineProfile 'XDHyp:
\HostingUnits\aws\w2022-2411
(lt-00123456789abcdef).launchtemplate\lt-00123456789abcdef
(1).launchtemplateversion' -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
00000000-0000-0000-0000-00000000000-HostingUnitName aws

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

Nota:

- Todas as especificações de versão de imagem em uma definição de imagem devem pertencer à mesma unidade de hospedagem.
- Uma versão de imagem pode ter apenas uma especificação de versão de imagem mestre e uma especificação de versão de imagem preparada.
- Todas as especificações de versão de imagem devem ter um perfil de máquina.

Compartilhar imagens preparadas entre zonas de disponibilidade e regiões

Agora você pode compartilhar uma única imagem preparada entre diferentes zonas de disponibilidade, vinculadas a diferentes unidades de hospedagem, dentro da mesma região AWS ou em regiões diferentes para seus ambientes AWS EC2. Isso permite que você use uma imagem preparada para criar e atualizar catálogos de máquinas MCS em várias zonas de disponibilidade e regiões. Ao compartilhar entre diferentes AZs em regiões diferentes, a versão da imagem preparada será copiada da região original para as regiões de destino.

Você pode manter uma única imagem preparada e usá-la para criar e atualizar catálogos de máquinas em várias zonas de disponibilidade e regiões vinculadas a diferentes unidades de hospedagem. Isso reduz significativamente a sobrecarga de gerenciamento de imagens, garante a consistência entre as implantações e simplifica o processo de provisionamento. Você também pode atualizar facilmente os catálogos de máquinas existentes com imagens preparadas de uma zona de disponibilidade ou região diferente.

Casos de uso

- **Gerenciamento Centralizado de Imagens:** Você cria uma imagem preparada em uma zona de disponibilidade (por exemplo, `us-east-1a`). Você pode então compartilhar esta imagem com outras zonas de disponibilidade como `us-east-1b` dentro da mesma região AWS `us-east-1` ou `us-west-1a` em uma região `us-west-1` diferente. Isso permite que uma única imagem atenda a várias unidades de hospedagem e simplifica a manutenção para você.
- **Criação e Atualização Eficientes de Catálogos:** Você pode usar uma imagem preparada criada em `AZ 1` (por exemplo, `us-east-1a`) para criar novos catálogos em `AZ 1`. Depois de compartilhar esta imagem com `AZ 2` (por exemplo, `us-east-1b`), você pode então usar a imagem compartilhada em `AZ 2` para criar e atualizar catálogos em `AZ 2`.
- **Implantações entre unidades de hospedagem e conexões de hospedagem:** Se seu ambiente tiver várias unidades de hospedagem na mesma ou em diferentes regiões AWS, você poderá compartilhar eficientemente imagens preparadas entre essas unidades de hospedagem.

Limitações

Compartilhamento dentro da mesma conta AWS: Na implementação atual, você pode compartilhar apenas dentro da mesma conta AWS.

Considerações importantes

- **Ordem de exclusão:** Para excluir uma especificação de versão de imagem preparada original, você deve primeiro excluir todas as suas especificações de versão de imagem compartilhadas.

Alternativamente, você deve excluir as especificações originais e compartilhadas simultaneamente.

- **Dependência da Versão da Imagem:** Ao remover uma versão da imagem, você deve primeiro remover quaisquer configurações de compartilhamento que dependam dessa versão específica da imagem. Os catálogos que você criou a partir da imagem original (não compartilhada) podem permanecer intactos.
- **Retrocompatibilidade do Catálogo:** Você pode atualizar catálogos de máquinas existentes que você implantou antes da introdução deste recurso. Use imagens preparadas que você criou em uma zona de disponibilidade ou região diferente daquela onde você implantou originalmente o catálogo.
- **Exclusão completa:** Ao excluir uma imagem preparada, você não poderá mais usá-la em nenhuma zona de disponibilidade onde a compartilhou ou a criou originalmente. Além disso, uma versão de imagem preparada não pode ser excluída até que todos os catálogos vinculados a essa versão de imagem preparada sejam excluídos primeiro.

Pré-requisitos

Antes de configurar ou usar este recurso, certifique-se de que você atende às seguintes condições:

- Seu ambiente deve ser um ambiente AWS EC2.
- Você deve configurar várias unidades de hospedagem (cada uma pode ser vinculada a diferentes zonas de disponibilidade) e conexões de host (cada uma pode ser vinculada a uma região diferente) na mesma conta AWS.

Configurar usando PowerShell

Atualmente, você pode compartilhar imagens preparadas entre zonas de disponibilidade vinculadas a diferentes unidades de hospedagem usando apenas comandos PowerShell.

PARA COMPARTILHAR UMA IMAGEM PREPARADA

1. Certifique-se de ter o `ImageVersionSpecUid` da imagem preparada que você deseja compartilhar. Você pode recuperá-lo usando `Get-ProvImageVersionSpec` ou comandos `Get-` semelhantes no PowerShell.
2. Determine o `HostingUnitName` da zona de disponibilidade (pode ser a mesma região ou uma região diferente) onde você deseja disponibilizar a imagem preparada. Este é o nome da unidade de hospedagem que você configurou para essa zona de disponibilidade específica.

3. **Execute o comando `Add-ProvImageVersionSpecHostingUnit`:** Use o seguinte comando PowerShell. Substitua `<ImageVersionSpecUid>` pelo Uid da sua imagem e `<targetHostingUnitName>` pelo nome da unidade de hospedagem na zona de disponibilidade de destino para a qual você deseja compartilhar a especificação da versão da imagem:

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
<ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
```

4. Após a execução bem-sucedida, você pode ver o status da imagem na interface do usuário do Studio, indicando que você a compartilhou com a unidade de hospedagem especificada.

PARA REMOVER O COMPARTILHAMENTO DE UMA IMAGEM PREPARADA

1. Certifique-se de ter o `ImageVersionSpecUid` da imagem preparada da qual você deseja remover o compartilhamento.
2. Determine o `HostingUnitName` da zona de disponibilidade da qual você deseja remover a imagem compartilhada.
3. **Execute o comando `Remove-ProvImageVersionSpecHostingUnit`:** Use o seguinte comando PowerShell. Substitua `<ImageVersionSpecUid>` pelo Uid da sua imagem e `<targetHostingUnitName>` pelo nome da unidade de hospedagem na zona de disponibilidade de destino da qual você deseja remover o compartilhamento da especificação da versão da imagem:

```
Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid
<ImageVersionSpecUid> -HostingUnitName <targetHostingUnitName>
```

Criar um catálogo de máquinas

Usar o Studio

CRIAR UM CATÁLOGO DE MÁQUINAS A PARTIR DO NÓ IMAGENS

Use a opção **Criar catálogo** no nó **Imagens** para criar um catálogo usando a versão da imagem.

Alternativamente, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de Máquinas**, vinculando à opção de imagem preparada no fluxo de trabalho de criação de catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas.

Para criar um catálogo de máquinas MCS a partir do nó **Imagens**, faça o seguinte:

1. Selecione uma versão da imagem e clique em **Criar catálogo**. Clique em **Avançar** na página **Introdução**.
2. Nas páginas **Gerenciamento de Máquinas** e **Imagem**, as configurações são pré-selecionadas com base na versão da imagem selecionada. Na página Imagem, insira uma nota para a imagem preparada selecionada.
3. Conclua as configurações nas páginas seguintes.
4. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.
5. Vá para o nó **Catálogos de Máquinas** para ver o catálogo de máquinas criado.

Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó Catálogos de Máquinas, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo.
2. Clique em **Criar Catálogo de Máquinas**. A página **Configuração do Catálogo de Máquinas** é exibida.
3. Na página **Tipo de Máquina**, selecione um tipo de máquina para o catálogo, por exemplo, **SO Multissessão**.
4. Na página **Gerenciamento de Máquinas**, selecione as seguintes configurações:
    a. Selecione **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade)**.
    b. Selecione **Tecnologia de provisionamento Citrix**. Em seguida, selecione **Citrix Machine Creation Services™**.
    c. No campo **Recursos**, selecione os recursos (Zona de Disponibilidade) que você configurou ao criar a conexão de host e clique em **Avançar**.
5. Na página **Experiência de desktop**, selecione um desktop aleatório ou estático que você deseja que os usuários tenham ao fazer login. Se um desktop estático for selecionado, especifique ainda se você deseja salvar as alterações que o usuário faz no disco local (persistente ou não persistente).
6. Na página **Imagem**, clique em **Selecionar uma imagem** para selecionar uma imagem preparada para o catálogo de máquinas. Selecione a versão preparada que você criou. Clique no nome da versão da imagem. Para ver mais detalhes sobre a versão da imagem selecionada, clique no número da versão, que está sublinhado. Clique em **Concluído**.

O perfil da máquina associado à imagem preparada aparece e suas propriedades de hardware (por exemplo, tipo de instância, tipo de locação, mapeamentos de rede, grupos de segurança, propriedades de volume) são usadas para criar máquinas nos catálogos. Para alterar a origem do perfil da máquina para outra VM ou versão de modelo de inicialização, clique no botão de edição.

7. Na página **Máquinas Virtuais**:
   a. Insira o número de VMs para o catálogo.
   b. A especificação padrão da máquina é exibida, que é baseada no perfil da máquina. Para alterá-la, selecione o ícone de edição e selecione uma especificação de máquina.
8. Na página **NICs**, selecione as NICs (ou ENIs) para as VMs.
9. Na página **Identidades da Máquina**, configure o Active Directory local ou o Microsoft Entra híbrido para as máquinas no catálogo, selecionando o domínio e criando novas contas AD para as VMs a serem criadas neste catálogo de máquinas. As VMs provisionadas são unidas ao domínio selecionado. Especifique o esquema de nomenclatura de conta para as novas contas AD a serem criadas para as VMs. Clique em **Avançar**.
10. Na página **Credenciais de domínio**, clique em **Inserir credenciais** para fornecer as credenciais para o domínio selecionado. Insira o nome de usuário e a senha de nível de administrador quando solicitado. Você também pode usar uma conta de serviço se já tiver credenciais de domínio salvas anteriormente, seguindo nossa documentação do produto.
11. Clique nas páginas restantes até a página **Resumo**. Insira um nome para o catálogo de máquinas e selecione **Concluir** para criar o catálogo de máquinas.

Usar PowerShell

CRIAR UM CATÁLOGO USANDO UMA ESPECIFICAÇÃO DE VERSÃO DE IMAGEM PREPARADA E UM PERFIL DE MÁQUINA

- Crie um catálogo de máquinas não persistentes do MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$true] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

- Crie um catálogo de máquinas persistentes do MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$false] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

Exemplo do conjunto completo de comandos PowerShell para criar um catálogo:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "awscatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "domainname"
-IdentityPoolName "awscatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "aws##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName awscatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName aws -IdentityPoolName awscatalog -CleanOnBoot -Scope @()
-SecurityGroup @() -MachineProfile 'XdHyp:\HostingUnits\cvad-test-
scalestress\us-east-1a.availabilityzone\machine-profile-instance i
(i-0xxxxxxx).vm' -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName awscatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Onde ir em seguida

- Gerenciar catálogos criados usando imagens preparadas

Mais informações

- Gerenciamento de imagens

Criar catálogos usando imagens preparadas no Azure

Crie imagens preparadas e use as imagens preparadas para criar um catálogo de máquinas MCS usando:

- Studio
- Comandos PowerShell

As etapas principais para criar um catálogo de máquinas MCS usando a imagem preparada são:

1. Crie a definição da imagem e as versões iniciais da imagem.
2. Use a versão da imagem como uma imagem preparada para criar um catálogo

Usar o Studio

Criar uma definição de imagem e a versão inicial da imagem

Para criar uma definição de imagem e a versão inicial da imagem, faça o seguinte:

1. No Studio, vá para o nó **Imagens** e clique em **Criar Definição de Imagem**. Clique em **Avançar** na página **Introdução**.
2. Na página **Definição de Imagem**, especifique o **Tipo de SO** e o **Tipo de Sessão** para a definição da imagem.
3. Selecione um grupo de recursos existente ou crie um novo para armazenar os recursos da imagem. Para habilitar o compartilhamento de imagens, selecione **Armazenar versões de imagem na Galeria de Computação do Azure** e, em seguida, escolha criar uma nova galeria ou usar uma existente para armazenar suas versões de imagem.
4. Na página **Imagem**, selecione **Recursos** (somente os recursos aplicáveis para a conexão definida são listados) e uma imagem mestre para usar como modelo para criar a versão da imagem. Você pode marcar a caixa de seleção **Usar um perfil de máquina** e selecionar um perfil de máquina.

> **Nota:**

- Antes de selecionar uma imagem, verifique se a imagem mestre tem o VDA 2311 ou posterior instalado e se o driver MCSIO está instalado no VDA.
- Se você quiser usar uma imagem preparada do tipo VM confidencial para criar um catálogo MCS, crie uma imagem preparada usando a imagem mestre do tipo VM confidencial e um perfil de máquina do tipo VM confidencial. Consulte VMs confidenciais do Azure para obter informações sobre como preparar imagens mestre e perfis de máquina do tipo VM confidencial.

5. Na página **Tipos de Armazenamento e Licenças**, selecione o tipo de armazenamento e licença a ser usado como parte do processo de preparação da imagem.

Nota:

Se você selecionar um perfil de máquina na página **Imagem**, o tipo de licença do perfil de máquina será pré-selecionado com base na configuração do perfil.

6. Na página **Especificação da Máquina**, selecione um tamanho de máquina. Se você selecionar um perfil de máquina na página **Imagem**, o tamanho da máquina do perfil de máquina será selecionado por padrão.
7. Na página **NICs**, selecione ou adicione NICs para a imagem de preparação. Para cada NIC, selecione uma rede virtual associada.
8. Na página **Configurações de Disco**, selecione a chave de criptografia gerenciada pelo cliente (CMEK). Se o perfil da máquina não tiver uma CMEK, mas a imagem mestre tiver, ele pré-selecionará a CMEK da imagem mestre.
9. Na página **Definição da Imagem**, se você habilitar **Armazenar versões de imagem na Galeria de Computação do Azure**, a página **Compartilhamento de Imagem** aparecerá, onde você pode selecionar os recursos com os quais compartilhar a versão da imagem.
10. Na página **Descrição da Versão**, insira uma descrição para a versão inicial da imagem criada.
11. Na página **Resumo**, verifique os detalhes da definição da imagem e da versão inicial da imagem criada. Insira um nome e uma descrição para a definição da imagem. Clique em **Concluir**.

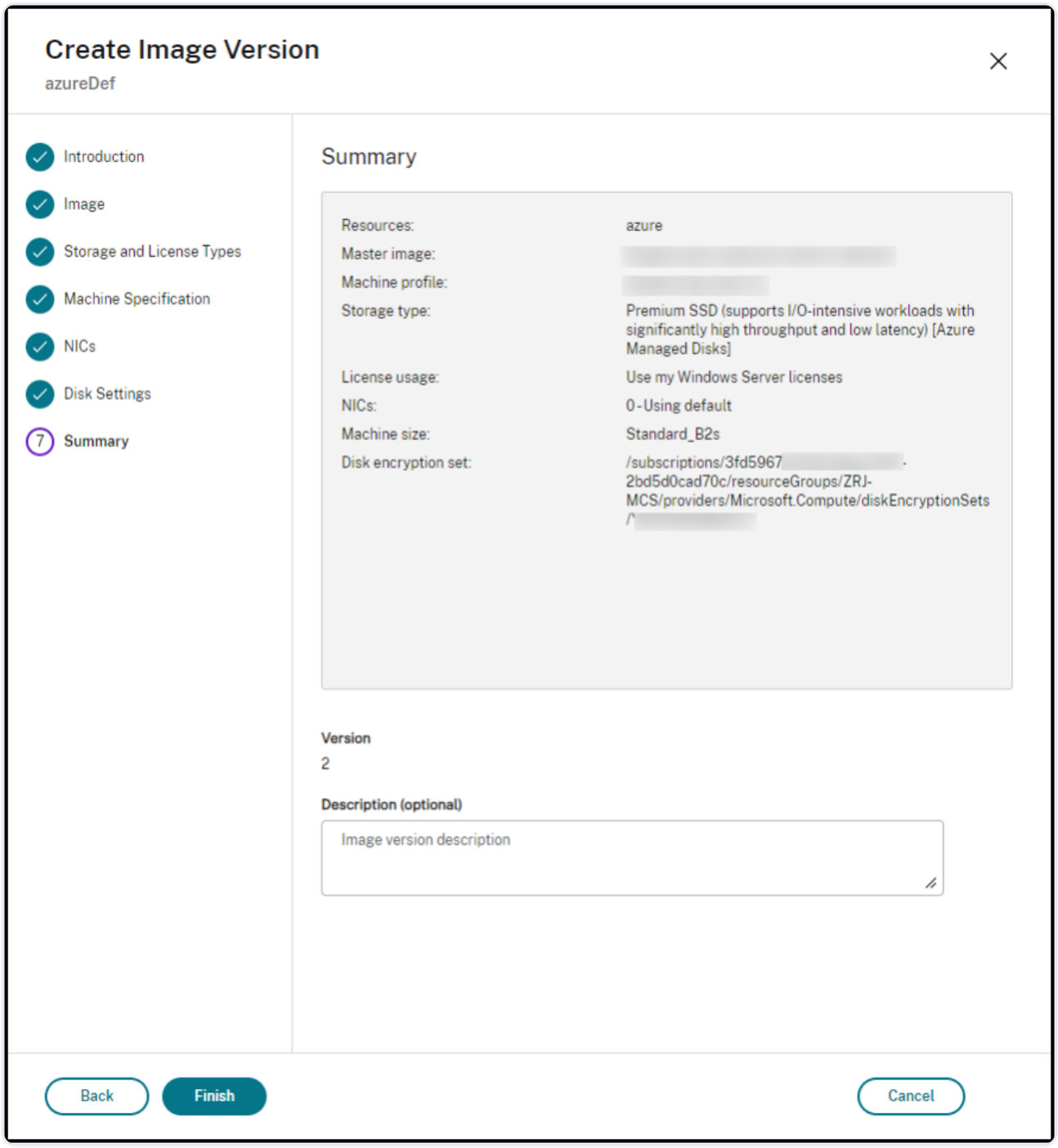
Criar versões de imagem

As versões de imagem permitem o gerenciamento de diferentes iterações ou atualizações para uma imagem específica. Essa funcionalidade permite que você mantenha várias versões de uma imagem para diferentes finalidades.

Para criar versões de imagem a partir da versão inicial da imagem, faça o seguinte:

> **Nota:**
>
> A unidade de hospedagem de todas as versões da imagem deve ser a mesma.

1. Vá para o nó **Imagens**, selecione uma versão de imagem ou uma definição de imagem e clique em **Criar Versão da Imagem**.
2. Na página de definição da imagem, você pode alterar a unidade de hospedagem e selecionar novamente a imagem mestre e o perfil da máquina para essa versão da imagem.
3. Se você quiser que a configuração da versão da imagem seja diferente da versão da imagem configurada inicialmente, configure as definições nas páginas **Tipos de Armazenamento e Licença**, **Especificação da Máquina**, **NICs** e **Configurações de Disco** da caixa de diálogo **Criar Versão da Imagem**.
4. Se a definição da imagem habilitar **Armazenar versões de imagem na Galeria de Computação do Azure**, você poderá selecionar os recursos com os quais deseja compartilhar a versão da imagem na página **Compartilhamento de Imagem**.
5. Adicione uma descrição para a versão da imagem. Clique em **Concluir**.



Nota:

Se a criação da versão da imagem falhar por qualquer motivo, a guia **Solução de problemas** na parte inferior fornecerá uma opção **Repetir**.

Compartilhar imagem preparada

Para compartilhar imagens preparadas entre diferentes unidades de hospedagem para o Azure, siga estas etapas:

1. Clique com o botão direito do mouse em uma versão da imagem e selecione **Gerenciar Compartilhamento de Imagem**. Todas as unidades de hospedagem em seu ambiente Azure aparecerão. Os recursos de onde a versão da imagem é criada são desabilitados para quaisquer ações.
2. Selecione as unidades de hospedagem com as quais você deseja compartilhar a imagem e clique em **Salvar**. A coluna **Status do Compartilhamento** mostra **Em andamento**.
3. Clique na guia **Recursos** para obter mais detalhes sobre o status do compartilhamento.

> **Nota:**
>
> Quando o status do compartilhamento da versão da imagem está em andamento, a opção **Excluir Versão da Imagem** ou **Gerenciar Compartilhamento de Imagem** é desabilitada.

Criar um catálogo de máquinas a partir do nó Imagens

Use a opção **Criar catálogo** no nó **Imagens** para criar um catálogo usando a versão da imagem.

Alternativamente, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de Máquinas**, vinculando à opção de imagem preparada no fluxo de trabalho de criação de catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Imagens**, faça o seguinte:

1. Selecione uma versão da imagem e clique em **Criar catálogo**. Clique em **Avançar** na página **Introdução**.
2. Na página **Experiência da Área de Trabalho**, selecione a experiência da área de trabalho necessária.
3. Da página **Imagem** à página **Configurações de Disco**, as configurações são pré-selecionadas com base na versão da imagem selecionada.
4. Na página **Grupo de Recursos**, você pode optar por criar um novo grupo de recursos ou usar um grupo de recursos existente para colocar os recursos deste catálogo.
5. Conclua as configurações nas páginas seguintes.
6. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.
7. Vá para o nó **Catálogos de Máquinas** para ver o catálogo de máquinas criado.

Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Catálogos de Máquinas**, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo.
2. Clique em **Criar Catálogo de Máquinas**. A página **Configuração do Catálogo de Máquinas** é exibida. Clique em **Avançar** nas páginas **Introdução** e **Tipo de Máquina**.
3. Na página **Gerenciamento de Máquinas**, selecione as seguintes configurações:
    a. Selecione **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade).**
    b. Selecione **Tecnologia de provisionamento Citrix**. Em seguida, selecione **Citrix Machine Creation Services™**.
    c. No campo **Recursos**, os recursos pertencentes a diferentes zonas são listados. Selecione qualquer recurso de rede do Azure e clique em **Avançar**.
4. Na página **Imagem**: Para o tipo de imagem Preparada, siga as etapas:
    a. Selecione **Imagem preparada**.
    b. Em **Imagem preparada**, selecione uma versão de imagem de uma definição de imagem. Se necessário, adicione uma nota para a versão da imagem preparada selecionada.
    c. Clique no nome da versão da imagem. Para ver mais detalhes sobre a versão da imagem selecionada, clique no número da versão, que está sublinhado.
    d. Se a versão da imagem selecionada estiver configurada com um perfil de máquina, selecione um perfil de máquina. Se a versão da imagem selecionada não estiver configurada com um perfil de máquina, você não poderá optar por usar um perfil de máquina.
5. Configure as configurações nas páginas a seguir.
6. Na página **Configurações de Disco**, se a imagem preparada selecionada usar um conjunto de criptografia de disco, você não poderá remover o conjunto de criptografia, mas poderá alterar a chave para outra chave de criptografia.
7. Na página **Grupo de Recursos**, você pode optar por criar um novo grupo de recursos ou usar um grupo de recursos existente para colocar os recursos deste catálogo.
8. Conclua as configurações nas páginas a seguir.
9. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.

Usar PowerShell

Criar uma imagem preparada

Os comandos detalhados do PowerShell para criar uma especificação de versão de imagem preparada são os seguintes:

1. Verifique os nomes de definição de imagem disponíveis usando `Test-ProvImageDefinitionNameAvailable command`. Por exemplo,

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. Crie uma definição de imagem usando o comando `New-ProvImageDefinition`. Por exemplo,

   ```
   New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
   -VdaSessionSupport MultiSession
   ```

3. Crie uma nova configuração para a definição de imagem na conexão de hospedagem especificada usando o comando `Add-ProvImageDefinitionConnection`.

   O `CustomProperties` para `Add-ProvImageDefinitionConnection` pode incluir o seguinte. Se você não usar os parâmetros, os valores padrão serão usados.

   - `ResourceGroups`: O grupo de recursos que possui os discos base.
   - `UseSharedImageGallery`: Indicador para o tipo de discos base. Use `true` para ACG (compartilhamento de imagem) e `false` para snapshot.
   - `ImageGallery`: O nome da galeria quando o disco base é uma versão de imagem ACG.

   Por exemplo,

   - No caso de snapshot e grupo de recursos fornecido pelo cliente:

     ```
     $CustomerOwnRsourceGroupProperties = @"

     <CustomProperties xmlns="http:// schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">

     <Property xsi:type="StringProperty" Name="ResourceGroups"
     Value="yangj_image" />
     ```

```
</CustomProperties>

"@
```

- No caso de ACG e grupo de recursos e galeria de imagens fornecidos pelo cliente:

```
$CustomerOwnAllProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

<Property xsi:type="StringProperty" Name="ImageGallery"
Value="gallery" />

</CustomProperties>

"@
```

- No caso de ACG e grupo de recursos fornecido pelo cliente apenas:

```
$CustomerOwnResourceGroupProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

</CustomProperties>
```

```
"@
```

- No caso de ACG e grupo de recursos e galeria de imagens gerenciados pela Citrix:

```
$CustomerOwnResourceGroupNothingProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

</CustomProperties>

"@
```

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 [-CustomProperties $CustomProperties]
```

4. Crie uma versão de imagem usando o comando `New-ProvImageVersion`. Por exemplo,

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. Adicione uma especificação de versão de imagem mestre à versão da imagem usando o comando `Add-ProvImageVersionSpec`. Por exemplo,

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
22-snapshot.snapshot"
```

Nota:

Você pode adicionar apenas uma especificação de versão de imagem mestre a uma versão de imagem para uma unidade de hospedagem.

6. Crie uma especificação de versão de imagem preparada a partir da especificação de versão de imagem mestre usando o comando `New-ProvImageVersionSpec`.

   As CustomProperties para `New-ProvImageVersionSpec` podem incluir o seguinte. Se você não usar os parâmetros, os valores padrão serão usados:

   - `PreparedImageStorageType`: O tipo de armazenamento a ser usado para a imagem preparada. O padrão é `Standard_LRS`, também pode ser `Premium_LRS` ou `Standard_ZRS`. `Standard_ZRS` fornece redundância de zona para a imagem.

   ```
   New-ProvImageVersionSpec

   -SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

   -NetworkMapping @{"0"="XDHyp:
   \HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
   rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"}

   -ServiceOffering"XDHyp:
   \HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
   g" -CustomProperties "<CustomProperties xmlns=`"http://
   schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
   www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
   -RunAsynchronously
   ```

7. Você também pode compartilhar uma especificação de versão de imagem preparada com outra unidade de hospedagem em todas as conexões de hospedagem usando o comando `Add-ProvImageVersionSpecHostingUnit`.

   As CustomProperties para `Add-ProvImageVersionSpecHostingUnit` podem incluir o seguinte. Se você não usar os parâmetros, os valores da especificação da imagem preparada de origem serão usados:

   - `PreparedImageStorageType`: O tipo de armazenamento a ser usado para a imagem preparada.

   ```
   Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
   -HostingUnitName AzureWest
   ```

> **Nota:**
>
> Uma unidade de hospedagem e tipo de preparação podem ter apenas uma instância preparada.

Exemplo do conjunto completo de comandos Powershell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession



$ImageDefinitionCustomProperties = @" <CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance"> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /> <Property
xsi:type="StringProperty" Name="ResourceGroups" Value="rg" /> <Property
xsi:type="StringProperty" Name="ImageGallery" Value="gallery" /> </
CustomProperties> "@



Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 -CustomProperties
$ImageDefinitionCustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid ` -HostingUnitUid
$hostingunit.HostingUnitUid ` -MasterImagePath "XDHyp:
\HostingUnits\azure28\image.folder\abc.resourcegroup\def-
snapshot.snapshot"
```

```
$ImageVersionSpecCustomProperties = @'



<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">



<Property xsi:type="StringProperty" Name="PreparedImageStorageType"
Value="Premium_LRS" />



<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />



</CustomProperties>



'@



New-ProvImageVersionSpec -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network" } -CustomProperties
$ImageVersionSpecCustomProperties -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
-SourceImageVersionSpecUid $SourceImageVersionSpec.ImageVersionSpecUid



$TargetCustomProperties = @'



<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
```

```
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">



<Property xsi:type="StringProperty" Name="PreparedImageStorageType"
Value="Standard_ZRS" />



</CustomProperties>



'@



Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest –TargetCustomProperties $TargetCustomProperties



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

Nota:

- Todas as especificações de versão de imagem em uma definição de imagem devem pertencer à mesma unidade de hospedagem.
- Uma versão de imagem pode ter apenas uma especificação de versão de imagem mestre e uma especificação de versão de imagem preparada.
- Todas as especificações de versão de imagem devem ter um perfil de máquina ou nenhuma das especificações de versão de imagem deve ter um perfil de máquina.

Criar um catálogo usando uma especificação de versão de imagem preparada

Crie um catálogo de máquinas MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]

[-ImageAssignmentNote <string>]
```

Ou,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]

[-ImageAssignmentNote <string>]
```

Se você quiser usar uma especificação de versão de imagem ACG, defina `UseSharedImageGallery` como `true`. Por exemplo,

```
$provSchemeCustomProperties= @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

    <Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" />

</CustomProperties>
```

```
"@

New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -IdentityPoolUid $IdentityPool.IdentityPoolUid `

    -CleanOnBoot -Scope @() -SecurityGroup @() `

    -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
`

    -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network"} `

    -CustomProperties $provSchemeCustomProperties
```

Exemplo do conjunto completo de comandos Powershell para criar um catálogo:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
```

```
$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">    <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /><Property
xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"StandardSSD_LRS`" /></CustomProperties>" -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Criar catálogos ingressados no Microsoft Entra e registrados no Microsoft Intune com imagens preparadas

Agora você pode usar imagens preparadas para criar catálogos ingressados no Microsoft Entra e registrados no Microsoft Intune. Este recurso é aplicável a catálogos MCS de tipo persistente e não persistente de sessão única e multi-sessão. Esta implementação reduz significativamente os custos de armazenamento e tempo, e simplifica o processo de implantação de VM e atualização de imagem.

EXEMPLOS

- Para criar um catálogo Microsoft Entra usando uma imagem preparada.

```
New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
<preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid>
-IdentityPoolUid <IdentityPoolUid> [-CleanOnBoot] -NetworkMapping
```

```
@{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.fol
der\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<s
unNetName>.network"} -ServiceOffering <serviceofferingPath> [-
MachineProfile <machineProfilePath>] [-CustomProperties <>]
```

- Para criar um catálogo Microsoft Entra registrado no Microsoft Intune usando uma imagem preparada:

```
New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
<preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid>
-IdentityPoolUid <IdentityPoolUid> [-CleanOnBoot] -NetworkMapping
@{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.fol
der\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<s
unNetName>.network"} -ServiceOffering <serviceofferingPath> [-
MachineProfile <machineProfilePath>] [-CustomProperties <>]
```

Compartilhar imagens preparadas entre assinaturas ou locatários do Azure

Para compartilhar uma imagem preparada entre assinaturas ou locatários na plataforma Azure, siga este exemplo:

- **Entidade de serviço**: SPN 1
- **Assinatura**: Subscription 1
- **Locatário**: Tenant 1

Você deseja compartilhar esta imagem com:

- **Entidade de serviço**: SPN 2
- **Assinatura**: Subscription 2
- **Locatário**: Tenant 2 (pode ser o mesmo que o Locatário 1)

Para compartilhar e usar a imagem com sucesso, você deve conceder ao SPN 2 as seguintes permissões na **Subscription 1** — no escopo da galeria, grupo de recursos ou assinatura:

- `Microsoft.Resources/subscriptions/read`
- `Microsoft.Compute/galleries/images/read`
- `Microsoft.Compute/galleries/images/versions/read`

> **Nota:**
>
> Qualquer entidade de serviço que tenha qualquer permissão em uma assinatura ou recurso herda automaticamente a permissão `Microsoft.Resources/subscriptions/read`.

Alternativamente, atribua a função interna de **Leitor de Imagem da Galeria de Computação** ao **SPN 2**.

Para obter orientação passo a passo, consulte este artigo da Microsoft.

Compartilhar imagem preparada criptografada entre regiões, assinaturas e locatários

As imagens da Azure Compute Gallery (ACG) podem ser criptografadas com um Conjunto de Criptografia de Disco (DES). Com o recurso de compartilhamento da ACG, você pode compartilhar uma imagem preparada criptografada entre regiões, assinaturas e locatários para o Azure. O recurso de destino precisa escolher um DES em sua região a partir da assinatura à qual a imagem preparada pertence. Você pode, então, criar um catálogo de máquinas no recurso onde a imagem preparada criptografada é compartilhada.

As etapas principais para compartilhar uma imagem preparada criptografada são:

1. Crie um Conjunto de Criptografia de Disco (DES) em cada região: Consulte a documentação da Microsoft Use o portal do Azure para habilitar a criptografia do lado do servidor com chaves gerenciadas pelo cliente para discos gerenciados.
2. Crie uma definição de imagem para a conexão do host do Azure e versões de imagem na Azure Compute Gallery (ACG) e especifique o DES para criptografar a imagem preparada: Consulte Criar uma definição de imagem e versão inicial da imagem.
3. Compartilhe a imagem preparada criptografada entre regiões, assinaturas e locatários: Você pode usar o Studio ou comandos do PowerShell.

Agora você pode criar um catálogo de máquinas no recurso onde a imagem preparada criptografada é compartilhada. Para obter mais informações sobre como criar o catálogo, consulte Criar um catálogo de máquinas de imagem preparada no Azure.

> **Nota:**

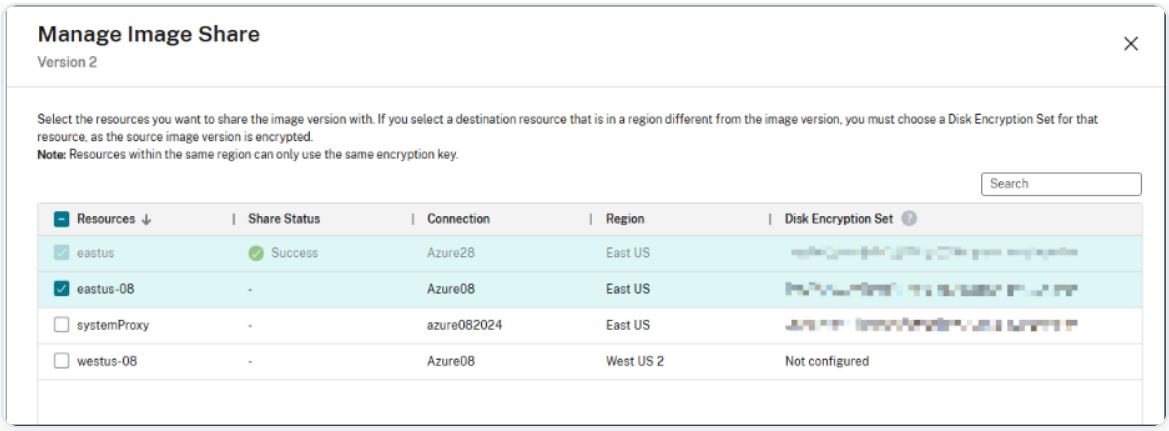
- Se a região primária não for criptografada, as regiões compartilhadas também não poderão ter DES.
- Se duas unidades de host visarem a mesma região, elas terão o mesmo DES.

Compartilhe a imagem criptografada entre regiões, assinaturas e locatários usando o Studio

1. Clique com o botão direito do mouse em uma versão da imagem e selecione **Gerenciar Compartilhamento de Imagem**. Os recursos com região e conjunto de criptografia de disco são listados.
2. Selecione os recursos que você deseja compartilhar com a versão da imagem. Os recursos de onde a versão da imagem é criada são desabilitados para quaisquer ações. Selecione um DES no menu suspenso se o DES não estiver configurado para um recurso.

Nota:

Os recursos dentro da mesma região devem usar a mesma chave de criptografia.



3. Clique em **Salvar**.
4. Clique na guia **Recursos** para obter mais detalhes sobre o status do compartilhamento.

Nota:

- Quando o status do compartilhamento da versão da imagem está em andamento, a opção **Excluir Versão da Imagem** ou **Gerenciar Compartilhamento de Imagem** é desabilitada.
- Quando um recurso é compartilhado com sucesso, o DES não é editável.

Compartilhe a imagem criptografada entre regiões, assinaturas e locatários usando o PowerShell

Use o comando `Add-ProvImageVersionSpecHostingUnit` e adicione o parâmetro `CustomProperties`. Em `CustomProperties`, configure o DES para o recurso de destino. Ao compartilhar a imagem criptografada preparada, cada recurso seleciona um DES em sua região a partir da assinatura à qual a imagem preparada pertence. Por exemplo,

```
$CustomProperties = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">"

 "<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/xxxxxx-7152-46c4-b061-xxxxxx70c/resourceGroups/
resourcegroup1/providers/Microsoft.Compute/diskEncryptionSets/desid1`" /
>"+

 "</CustomProperties>"

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <Guid>
-HostingUnitUid <Guid> -CustomProperties $CustomProperties
```

Mais informações

- Gerenciamento de imagens

Onde ir em seguida

- Gerenciar catálogos criados usando imagens preparadas

Criar catálogos usando imagens preparadas no Nutanix AHV Prism Central

Crie imagens preparadas e use as imagens preparadas para criar um catálogo de máquinas MCS usando:

- Comandos PowerShell

As etapas principais para criar um catálogo de máquinas MCS usando a imagem preparada são:

1. Crie a definição da imagem e as versões iniciais da imagem.
2. Use a versão da imagem como uma imagem preparada para criar um catálogo

Usar PowerShell

Exemplo de PowerShell do fluxo de trabalho de desacoplamento de imagem no Nutanix PC.

Configuração

```
$CustomProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"><StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378"/></CustomProperties>'

$MasterImagePath="XDHyp:\HostingUnits\${HostingUnitName}
\Templates.folder\hai-vda-novtpm01.template\Initial
Version.templateversion"

$VMNetwork1A="XDHyp:\HostingUnits\${HostingUnitName}\Clusters.folder\mcs-
pvs-ntnx-cluster01.cluster\vmNwCl1-A.network"

$NetworkMapping=@{"0"=$VMNetwork1A}
```

Criar definição de imagem e versão de imagem

```
$ImageDefinition = New-ProvImageDefinition -ImageDefinitionName
$ImgDefName -OsType Windows -VdaSessionSupport SingleSession

$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefinition.ImageDefinitionName -Description "V1"

Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefinition.ImageDefinitionName -HypervisorConnectionName
$HostingConnection
```

Criar especificação de versão de imagem

```
$MasterImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName $HostingUnitName
-MasterImagePath $MasterImagePath
```

```
$ProvTask = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $MasterImageVersionSpec.ImageVersionSpecUid -NetworkMapping
$NetworkMapping -MachineProfile $MachineProfile -CustomProperties
$CustomProperties -AdditionalStorageIds
00062c6d-09a3-134b-446d-58a2e17d0f88 -RunAsynchronously

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
$ImgDefName -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
```

Criar Esquema de Provisionamento

```
$ProvTask = New-ProvScheme -ProvisioningSchemeName $ProvSchemeName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName $HostingUnitName -IdentityPoolName $IdentityPoolName
-CleanOnBoot -Scope @() -SecurityGroup @() -NetworkMapping $NetworkMapping
-CustomProperties $CustomProperties -MachineProfile $MachineProfile
-RunAsynchronously
```

Replicar a especificação da versão da imagem para um novo cluster

```
Add-ProvImageVersionSpecInstance -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -StorageID
00062c6d-09a3-134b-446d-58a2e17d0f88
```

Criar um novo esquema de provisionamento no novo cluster usando a mesma imagem preparada

```
$CustomProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"><StringProperty Name="ClusterId"
Value="00062c6d-09a3-134b-446d-58a2e17d0f88"/></CustomProperties>'

$ProvTask = New-ProvScheme -ProvisioningSchemeName $ProvSchemeName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-MachineProfile $MachineProfile -HostingUnitName $HostingUnitName
-IdentityPoolName $IdentityPoolName -CleanOnBoot -Scope @() -SecurityGroup
@() -NetworkMapping $NetworkMapping -CustomProperties $CustomProperties
-RunAsynchronously
```

Mais informações

- Gerenciamento de imagens

Onde ir em seguida

- Gerenciar catálogos criados usando imagens preparadas

Criar catálogos usando imagens preparadas no Red Hat OpenShift

Crie imagens preparadas e use as imagens preparadas para criar um catálogo de máquinas MCS usando:

- Studio
- Comandos PowerShell

As etapas principais para criar um catálogo de máquinas MCS usando a imagem preparada são:

1. Crie a definição da imagem e as versões iniciais da imagem.
2. Use a versão da imagem como uma imagem preparada para criar um catálogo

Usar o Studio

Criar uma definição de imagem e a versão inicial da imagem

Para criar uma definição de imagem e a versão inicial da imagem, faça o seguinte:

1. No Studio, vá para o nó **Imagens** e clique em **Criar Definição de Imagem**. Clique em **Avançar** na página **Introdução**.
2. Na página **Definição de Imagem**, especifique o **Tipo de SO** e o **Tipo de Sessão** para a definição de imagem.
3. Na página **Imagem**, selecione **Recursos** (somente os recursos aplicáveis para a conexão definida são listados) e uma imagem mestre para usar como modelo para criar a versão da imagem. Você pode marcar a caixa de seleção **Usar um perfil de máquina** e selecionar um perfil de máquina.

   > **Nota:**
   >
   > Antes de selecionar uma imagem, verifique se a imagem mestre tem o VDA 2311 ou posterior instalado e se o driver MCSIO está instalado no VDA.

4. Na página **Especificação da Máquina**, selecione um tamanho de máquina. Se você selecionar um perfil de máquina, poderá ver a contagem de CPU Virtual derivada do perfil de

máquina e ela será imutável. Se você não selecionar um perfil de máquina, poderá ver apenas o tamanho da memória derivado da imagem mestre.

5. Na página **NICs**, selecione NICs para a imagem de preparação. Para cada NIC, selecione uma rede virtual associada. A NIC associada à unidade de hospedagem é selecionada por padrão.
6. Na página **Descrição da Versão**, insira uma descrição para a versão inicial da imagem criada.
7. Na página **Resumo**, verifique os detalhes da definição da imagem e da versão inicial da imagem criada. Insira um nome e uma descrição para a definição da imagem. Clique em **Concluir**.

Criar versões de imagem

As versões de imagem permitem o gerenciamento de diferentes iterações ou atualizações para uma imagem específica. Essa funcionalidade permite manter várias versões de uma imagem para diferentes finalidades.

Para criar versões de imagem a partir da versão inicial da imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma versão de imagem ou uma definição de imagem e clique em **Criar Versão da Imagem**.
2. Na página **Imagem**, você pode selecionar novamente a imagem mestre para esta versão da imagem.
3. Se você quiser que a configuração da versão da imagem seja diferente da versão inicial da imagem configurada, configure as definições nas páginas **Especificação da Máquina** e **NICs** da caixa de diálogo **Criar Versão da Imagem**.
4. Adicione uma descrição para a versão da imagem. Clique em **Concluir**.

> **Nota:**
>
> Se a criação da versão da imagem falhar por qualquer motivo, a guia **Solução de Problemas** na parte inferior fornece uma opção **Repetir**.

Criar um catálogo de máquinas a partir do nó Imagens

Use a opção **Criar catálogo** no nó **Imagens** para criar um catálogo usando a versão da imagem.

Alternativamente, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de Máquinas**, vinculando à opção de imagem preparada no fluxo de trabalho de criação de catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Imagens**, faça o seguinte:

1. Selecione uma versão de imagem e clique em **Criar catálogo**. Clique em **Avançar** na página **Introdução**.
2. Clique em **Avançar** na página **Gerenciamento de Máquinas**.
3. Na página **Experiência de Área de Trabalho**, selecione a experiência de área de trabalho necessária.
4. Da página **Imagem** à página **Máquinas Virtuais**, as configurações são pré-selecionadas com base na versão da imagem selecionada.
5. Conclua as configurações nas páginas seguintes.
6. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.
7. Vá para o nó **Catálogos de Máquinas** para ver o catálogo de máquinas criado.

Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Catálogos de Máquinas**, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo.
2. Clique em **Criar Catálogo de Máquinas**. A página **Configuração do Catálogo de Máquinas** é exibida. Clique em **Avançar** nas páginas **Introdução**, **Tipo de Máquina** e **Gerenciamento de Máquinas**.
3. Na página **Imagem**:
    a. Selecione **Imagem preparada**.
    b. Em **Imagem preparada**, selecione uma versão de imagem de uma definição de imagem.
    c. Clique no nome da versão da imagem. Para ver mais detalhes sobre a versão da imagem selecionada, clique no número da versão, que está sublinhado.
4. Configure as configurações nas páginas a seguir.
5. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.

Usar PowerShell

Criar uma imagem preparada

Os comandos detalhados do PowerShell para criar uma especificação de versão de imagem preparada são os seguintes:

1. Verifique os nomes de definição de imagem disponíveis usando o `Test-ProvImageDefinitionNameAvailable command`. Por exemplo,

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. Crie uma definição de imagem usando o comando `New-ProvImageDefinition`. Por exemplo,

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport SingleSession
```

3. Crie uma nova configuração para a definição de imagem na conexão de hospedagem especificada usando o comando `Add-ProvImageDefinitionConnection`. Por exemplo,

```
Add-ProvImageDefinitionConnection -ImageDefinitionUid
$imageDef.ImageDefinitionUid -HypervisorConnectionUid
"00000000-0000-0000-0000-000000000000"
```

4. Crie uma versão de imagem usando o comando `New-ProvImageVersion`. Por exemplo,

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. Adicione uma especificação de versão de imagem mestre à versão da imagem usando o comando `Add-ProvImageVersionSpec`. Por exemplo,

```
Add-ProvImageVersionSpec -MasterImagePath "XDHyp:
\HostingUnits\YourHostingUnitName\YourMasterImage.vm" -HostingUnitUid
"11111111-1111-1111-1111-111111111111" -ImageVersionUid
$imageVersion.ImageVersionUid
```

Nota:

Você pode adicionar apenas uma especificação de versão de imagem mestre a uma versão de imagem para uma unidade de hospedagem.

6. Crie uma especificação de versão de imagem preparada a partir da especificação de versão de imagem mestre usando o comando `New-ProvImageVersionSpec`. Por exemplo,

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
$masterImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"1" =
"XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetwo
rkAttachmentDefinition.network" }
```

Exemplo do conjunto completo de comandos Powershell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada:

```
$imageDef = New-ProvImageDefinition -ImageDefinitionName "ImageDefinition"
-OsType "Windows" -VDASessionSupport "MultiSession"




$task = Add-ProvImageDefinitionConnection -ImageDefinitionUid
$imageDef.ImageDefinitionUid -HypervisorConnectionUid
"00000000-0000-0000-0000-000000000000"



$imageVersion = New-ProvImageVersion -ImageDefinitionName
"ImageDefinition"




$masterImageVersionSpec = Add-ProvImageVersionSpec -MasterImagePath
"XDHyp:\HostingUnits\YourHostingUnitName\YourMasterImage.vm"
-HostingUnitUid "11111111-1111-1111-1111-111111111111" -ImageVersionUid
$imageVersion.ImageVersionUid




$newProvImageVersionSpecResult = New-ProvImageVersionSpec
```

```
-SourceImageVersionSpecUid $masterImageVersionSpec.ImageVersionSpecUid
-NetworkMapping @{"1" = "XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetworkA
ttachmentDefinition.network" }
```

Nota:

- Todas as especificações de versão de imagem em uma definição de imagem devem pertencer à mesma unidade de hospedagem.
- Uma versão de imagem pode ter apenas uma especificação de versão de imagem mestre e uma especificação de versão de imagem preparada.
- Todas as especificações de versão de imagem devem ter um perfil de máquina ou nenhuma das especificações de versão de imagem deve ter um perfil de máquina.

Criar um catálogo usando uma especificação de versão de imagem preparada

Crie um catálogo de máquinas MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
$getProvImageVersionSpecResult = Get-ProvImageVersionSpec
-ImageVersionSpecUid $newProvImageVersionSpecResult.ImageVersionSpecUid



New-ProvScheme -ImageVersionSpecUid
$newProvImageVersionSpecResult.ImageVersionSpecUid -ProvisioningSchemeName
"ProvSchemeImageDecoupling" -HostingUnitName "YourHostingUnitName"
-IdentityPoolName "YourIdentityPoolName" -NetworkMapping @{"1" = "XDHyp:
\HostingUnits\YourHostingUnitName\YourNamespaceName.namespace\YourNetworkA
ttachmentDefinition.network"}
```

Mais informações

- Gerenciamento de imagens

Onde ir a seguir

- Gerenciar catálogos criados usando imagens preparadas

Criar catálogos usando imagens preparadas no VMware

Crie imagens preparadas e use as imagens preparadas para criar um catálogo de máquinas MCS usando:

- Studio
- Comandos PowerShell

As etapas principais para criar um catálogo de máquinas MCS usando a imagem preparada são:

1. Crie a definição da imagem e as versões iniciais da imagem.
2. Use a versão da imagem como uma imagem preparada para criar um catálogo

Usar o Studio

Criar uma definição de imagem e a versão inicial da imagem

Para criar uma definição de imagem e a versão inicial da imagem, faça o seguinte:

1. No Studio, vá para o nó **Imagens** e clique em **Criar Definição de Imagem**. Clique em **Avançar** na página **Introdução**.
2. Na página **Definição de Imagem**, especifique o **Tipo de SO** e o **Tipo de Sessão** para a definição de imagem e a **Conexão** para a definição de imagem.
3. Na página **Imagem**, selecione **Recursos** (somente os recursos aplicáveis para a conexão definida são listados) e uma imagem mestre para usar como modelo para criar a versão da imagem. Você pode marcar a caixa de seleção **Usar um perfil de máquina** e selecionar um perfil de máquina.

   > **Nota:**
   >
   > Antes de selecionar uma imagem, verifique se a imagem mestre tem o VDA 2311 ou posterior instalado e se o driver MCSIO está instalado no VDA.

4. Na página **Especificação da Máquina**, selecione um tamanho de máquina. Se você selecionar um perfil de máquina, poderá ver a contagem de CPU Virtual derivada do perfil de máquina e ela será imutável. Se você não selecionar um perfil de máquina, poderá ver apenas o tamanho da memória derivado da imagem mestre.
5. Na página **NICs**, selecione ou adicione NICs para a imagem de preparação. Para cada NIC, selecione uma rede virtual associada. Se você não selecionar um perfil de máquina, a NIC

associada à imagem mestre será selecionada por padrão. Se você selecionar um perfil de máquina, as NICs serão derivadas do perfil de máquina e a contagem será imutável.

6. Na página **Descrição da Versão**, insira uma descrição para a versão inicial da imagem criada.
7. Na página **Resumo**, verifique os detalhes da definição da imagem e da versão inicial da imagem criada. Insira um nome e uma descrição para a definição da imagem. Clique em **Concluir**.

Criar versões de imagem

As versões de imagem permitem o gerenciamento de diferentes iterações ou atualizações para uma imagem específica. Essa funcionalidade permite manter várias versões de uma imagem para diferentes finalidades.

Para criar versões de imagem a partir da versão inicial da imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma versão de imagem ou uma definição de imagem e clique em **Criar Versão da Imagem**.
2. Na página **Imagem**, você pode alterar a unidade de hospedagem dentro da mesma conexão de hospedagem e selecionar novamente a imagem mestre e o perfil da máquina para essa versão da imagem.
3. Se você quiser que a configuração da versão da imagem seja diferente da versão inicial da imagem configurada, configure as definições nas páginas **Especificação da Máquina** e **NICs** da caixa de diálogo **Criar Versão da Imagem**.
4. Adicione uma descrição para a versão da imagem. Clique em **Concluir**.

> **Nota:**
>
> Se a criação da versão da imagem falhar por qualquer motivo, a guia **Solução de Problemas** na parte inferior fornecerá uma opção de **Repetir**.

Compartilhar imagens preparadas

PRÉ-REQUISITOS

Compartilhar imagens preparadas replica imagens entre instâncias do vCenter Server usando migração a frio. Os seguintes pré-requisitos se aplicam às unidades de hospedagem pertencentes a diferentes conexões de hospedagem:

- Conectividade do Cloud Connector com o vCenter de destino: O Cloud Connector do Local de Recurso de origem deve ter acesso HTTPS (porta 443) ao vCenter de destino. A replicação falha se o conector de origem não conseguir estabelecer uma conexão do SDK do vSphere para coordenar a operação.

ORIGEM	DESTINO	PORTA	PROTOCOLO	FINALIDADE
Cloud Connector de Origem	vCenter Server de Destino	443	TCP	Conexão de gerenciamento do SDK do vSphere

- Migração a frio entre vCenter Servers: A migração a frio requer suporte à migração entre vCenters em ambos os ambientes.
  - Ambos os vCenter Servers devem executar o vSphere 7.0 ou posterior (vSphere 8.0+ recomendado).
  - O modo vinculado aprimorado não é necessário.

  Requisito de porta: Certifique-se de que as seguintes portas estejam abertas para a migração:

ORIGEM	DESTINO	PORTA	PROTOCOLO	FINALIDADE
Servidor vCenter de Origem	Servidor vCenter de Destino	443	TCP	Comunicação de API entre vCenters
Host ESXi de Origem	Host ESXi de Destino	902	TCP	Transferência de dados NFC (Network File Copy)
Host ESXi de origem	Host ESXi de destino	8000	TCP	Tráfego vMotion

> **Observação:**

> As portas devem estar abertas bidirecionalmente. A migração usa principalmente NFC (porta 902) para dados e a porta 443 para gerenciamento. A porta 8000 pode ser usada

> dependendo do caminho. O vCenter de origem deve validar a impressão digital do certificado SSL do destino durante a operação de clonagem.

> Configuração do adaptador VMkernel:

HOST ESXI	SERVIÇO NECESSÁRIO
Host ESXi de origem	Provisionamento ou Gerenciamento
Host ESXi de destino	Mesmo serviço que a origem (Provisionamento ou Gerenciamento)

Ambos os lados devem habilitar o mesmo serviço de tráfego (Provisionamento ou Gerenciamento) nos adaptadores VMkernel. Incompatibilidades causam falha na migração.

Verifique no vSphere Client em **Host > Configure > Networking > VMkernel adapters**.

Limitação conhecida: As políticas de armazenamento personalizadas não são preservadas durante a replicação entre vCenters. A política de armazenamento padrão do datastore de destino é aplicada.

- Perfil de máquina habilitado para vTPM: Compatibilidade do provedor de chaves. Para perfis com vTPM, ambos os vCenter Servers devem acessar um Provedor de Chaves compatível.

REQUISITO	DETALHE
Mesmo acesso ao Provedor de Chaves	O vCenter de destino deve ter acesso ao mesmo provedor de chaves que a origem, ou usar o Provedor de Chaves Nativo como uma ponte
Material da chave	Para KMS externo: ambos os vCenters devem ser registrados no mesmo cluster KMS (ou em um cluster KMS que compartilhe o material da chave)
Provedor de Chaves Nativo	Configure um Provedor de Chaves Nativo em ambos os vCenter Servers. O Provedor de Chaves Nativo de cada vCenter é independente, mas o vSphere aceita essa combinação para operações entre vCenters. O Provedor de Chaves Nativo também pode

REQUISITO	DETALHE
	atuar como uma ponte se a origem e o destino não compartilharem um KMS externo. O Provedor de Chaves Nativo deve ser feito backup em ambos os vCenters antes do uso.

> **Nota:**
>
> O Provedor de Chaves Nativo é a opção mais simples. Configure-o e faça backup em ambos os servidores. Se estiver usando KMS externo, certifique-se de que ambos os vCenters compartilhem o mesmo cluster ou material de chave. Verifique a configuração do Provedor de Chaves no **vSphere Client em vCenter > Configure > Security > Key Providers antes de habilitar o compartilhamento de imagens para catálogos habilitados para vTPM**.

COMPARTILHAR IMAGENS PREPARADAS ENTRE DIFERENTES UNIDADES DE HOST

Para compartilhar imagens preparadas entre diferentes unidades de host, siga estas etapas:

1. Clique com o botão direito do mouse em uma versão da imagem e selecione **Gerenciar Compartilhamento de Imagem**. Todas as unidades de hospedagem em seu ambiente VMware aparecem. Os recursos de onde a versão da imagem foi criada são desabilitados para qualquer ação.
2. Selecione as unidades de hospedagem com as quais você deseja compartilhar a imagem e clique em **Salvar**. A coluna **Status do Compartilhamento** mostra **Em andamento**.
3. Clique na guia **Recursos** na parte inferior para obter mais detalhes sobre o status do compartilhamento.

> **Nota:**
>
> Quando o status do compartilhamento da versão da imagem está em andamento, a opção **Excluir Versão da Imagem** ou **Gerenciar Compartilhamento de Imagem** é desabilitada. Para compartilhar uma imagem com uma unidade de hospedagem em uma conexão VMware diferente, certifique-se de que os seguintes requisitos sejam atendidos:

- As duas conexões podem se comunicar entre si. As versões do hypervisor são consistentes.
- Os serviços de Provisionamento estão habilitados nos adaptadores VMkernel de gerenciamento dos hosts de origem e de destino. O caminho de navegação no VMware vSphere Client é **Host > Configurar > Rede > Adaptadores VMkernel**.

Criar um catálogo de máquinas a partir do nó Imagens

Use a opção **Criar catálogo** no nó **Imagens** para criar um catálogo usando a versão da imagem.

Alternativamente, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de Máquinas**, vinculando à opção de imagem preparada no fluxo de trabalho de criação de catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Imagens**, faça o seguinte:

1. Selecione uma versão da imagem e clique em **Criar catálogo**. Clique em **Avançar** na página **Introdução**.
2. Na página **Experiência de Área de Trabalho**, selecione a experiência de área de trabalho necessária.
3. Da página **Imagem** para a página **Máquinas Virtuais**, as configurações são pré-selecionadas com base na versão da imagem selecionada.
4. Conclua as configurações nas páginas a seguir.
5. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.
6. Vá para o nó **Catálogos de Máquinas** para ver o catálogo de máquinas criado.

Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Catálogos de Máquinas**, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo.
2. Clique em **Criar Catálogo de Máquinas**. A página **Configuração do Catálogo de Máquinas** é exibida. Clique em **Avançar** nas páginas **Introdução**, **Tipo de Máquina** e **Gerenciamento de Máquinas**.
3. Na página **Imagem**:
    a. Selecione **Imagem preparada**.

b. Em **Imagem preparada**, selecione uma versão de imagem de uma definição de imagem. Se necessário, adicione uma nota para a versão de imagem preparada selecionada.

c. Clique no nome da versão da imagem. Para ver mais detalhes sobre a versão da imagem selecionada, clique no número da versão, que está sublinhado.

d. Se a versão da imagem selecionada estiver configurada com um perfil de máquina, selecione um perfil de máquina. Se a versão da imagem selecionada não estiver configurada com um perfil de máquina, você não poderá optar por usar um perfil de máquina.

4. Configure as definições nas páginas a seguir.
5. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.

Usar PowerShell

Criar uma imagem preparada

Os comandos detalhados do PowerShell para criar uma especificação de versão de imagem preparada são os seguintes:

1. Verifique os nomes de definição de imagem disponíveis usando `Test-ProvImageDefinitionNameAvailable command`. Por exemplo,

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. Crie uma definição de imagem usando o comando `New-ProvImageDefinition`. Por exemplo,

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport SingleSession
```

3. Crie uma nova configuração para a definição de imagem na conexão de hospedagem especificada usando o comando `Add-ProvImageDefinitionConnection`. Por exemplo,

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware
```

4. Crie uma versão de imagem usando o comando `New-ProvImageVersion`. Por exemplo,

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. Adicione uma especificação de versão de imagem mestre à versão de imagem usando o comando `Add-ProvImageVersionSpec`. Por exemplo,

```
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware
-MasterImagePath $MasterImagePath
```

Nota:

Você pode adicionar apenas uma especificação de versão de imagem mestre a uma versão de imagem para uma unidade de hospedagem.

6. Crie uma especificação de versão de imagem preparada a partir da especificação de versão de imagem mestre usando o comando `New-ProvImageVersionSpec`. Por exemplo,

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. Você também pode compartilhar uma especificação de versão de imagem preparada com outra unidade de hospedagem dentro da mesma conexão de hospedagem usando o comando `Add-ProvImageVersionSpecHostingUnit`. Por exemplo,

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc
```

Exemplo do conjunto completo de comandos do Powershell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada:

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport Single



Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware



$imageVersion = New-ProvImageVersion -ImageDefinitionName image2



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\vmware\shuaiz-win10-
master.vm\shuaiz-win10-master-snap.snapshot"



New-ProvImageVersionSpec -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-
VMNetwork.network"} `

    -VMCpuCount 2 -VMMemoryMB 4096







Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc

 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

Nota:

- Todas as especificações de versão de imagem em uma definição de imagem devem pertencer à mesma unidade de hospedagem.
- Uma versão de imagem pode ter apenas uma especificação de versão de imagem mestre e uma especificação de versão de imagem preparada.
- Todas as especificações de versão de imagem devem ter um perfil de máquina ou nenhuma das especificações de versão de imagem deve ter um perfil de máquina.

Criar um catálogo usando uma especificação de versão de imagem preparada

Crie um catálogo de máquinas MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]

[-ImageAssignmentNote <string>]
```

Ou,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

```
[-ImageAssignmentNote <string>]
```

Exemplo de criação de um catálogo usando uma especificação de versão de imagem preparada no VMware:

```
New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitName $hostingunit.c-IdentityPoolName
$IdentityPool.IdentityPoolName `

    -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM
Network.network"}
```

Exemplo do conjunto completo de comandos Powershell para criar um catálogo:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId
```

```
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Mais informações

- Gerenciamento de imagens

Onde ir em seguida

- Gerenciar catálogos criados usando imagens preparadas

Criar catálogos usando imagens preparadas no XenServer®

Crie imagens preparadas e use as imagens preparadas para criar um catálogo de máquinas MCS usando:

- Studio
- Comandos do PowerShell

As etapas principais para criar um catálogo de máquinas MCS usando a imagem preparada são:

1. Crie a definição da imagem e as versões iniciais da imagem.
2. Use a versão da imagem como uma imagem preparada para criar um catálogo

Usar o Studio

Criar uma definição de imagem e a versão inicial da imagem

Para criar uma definição de imagem e a versão inicial da imagem, faça o seguinte:

1. No Studio, vá para o nó **Imagens** e clique em **Criar Definição de Imagem**. Clique em **Avançar** na página **Introdução**.
2. Na página **Definição de Imagem**, especifique o **tipo de SO** e o **tipo de sessão**, e a **Conexão** para a definição da imagem.
3. Na página **Imagem**, selecione **Recursos** (somente os recursos aplicáveis para a conexão definida são listados) e uma imagem mestre para usar como modelo para criar a versão da imagem.

> **Nota:**

- Antes de selecionar uma imagem, verifique se a imagem mestre tem o VDA 2311 ou posterior instalado e se o driver MCSIO está instalado no VDA.

4. Na página **Especificação da Máquina**, você pode ver apenas o tamanho da memória derivado da imagem mestre e pode alterá-lo se necessário.
5. Na página **NICs**, selecione as NICs para a imagem de preparação. Para cada NIC, selecione uma rede virtual associada. A NIC associada à imagem mestre é selecionada por padrão.
6. Na página **Descrição da Versão**, insira uma descrição para a versão inicial da imagem criada.
7. Na página **Resumo**, verifique os detalhes da definição da imagem e da versão inicial da imagem criada. Insira um nome e uma descrição para a definição da imagem. Clique em **Concluir**.

Criar versões de imagem

As versões de imagem permitem o gerenciamento de diferentes iterações ou atualizações de uma imagem específica. Essa funcionalidade permite manter várias versões de uma imagem para diferentes finalidades.

Para criar versões de imagem a partir da versão inicial da imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma versão de imagem ou uma definição de imagem e clique em **Criar Versão da Imagem**.
2. Na página **Imagem**, altere a unidade de hospedagem e selecione novamente a imagem mestre, se necessário.
3. Para usar configurações diferentes da versão inicial da imagem, configure as configurações nas páginas **Especificação da Máquina** e **NICs** na caixa de diálogo **Criar Versão da Imagem**.
4. Adicione uma descrição para a versão da imagem. Clique em **Concluir**.

Nota:

Se a criação da versão da imagem falhar por qualquer motivo, a guia **Solução de problemas** na parte inferior fornece uma opção **Tentar novamente**.

Imagem preparada compartilhada

Para compartilhar imagens preparadas entre diferentes unidades de host para XenServer, siga estas etapas:

1. Clique com o botão direito em uma versão da imagem e selecione **Gerenciar Compartilhamento de Imagem**. Todas as unidades de host sob a conexão selecionada são listadas. Os recursos de onde a versão da imagem é criada são desabilitados para quaisquer ações.
2. Selecione as unidades de host com as quais você deseja compartilhar a imagem e clique em **Salvar**. A coluna **Status do Compartilhamento** mostra **Em andamento**.
3. Clique na guia **Recursos** para obter mais detalhes sobre o status do compartilhamento.

> **Nota:**
>
> Quando o status do compartilhamento da versão da imagem está em andamento, a opção de excluir a versão da imagem ou gerenciar o compartilhamento da imagem é desabilitada.

Criar um catálogo de máquinas a partir do nó Imagens

Use a opção **Criar catálogo** no nó **Imagens** para criar um catálogo usando a versão da imagem.

Alternativamente, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de Máquinas**, vinculando à opção de imagem preparada no fluxo de trabalho de criação de catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Imagens**, faça o seguinte:

1. Selecione uma versão da imagem e clique em **Criar catálogo**. Clique em **Avançar** na página **Introdução**.
2. Na página **Gerenciamento de Máquinas**, selecione a unidade de hospedagem e clique em **Avançar**.
3. Na página **Experiência de Área de Trabalho**, selecione a experiência de área de trabalho necessária.
4. Da página **Imagem** para a página **Máquinas Virtuais**, as configurações são pré-selecionadas com base na versão da imagem selecionada.
5. Conclua as configurações nas páginas seguintes.

6. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.
7. Vá para o nó **Catálogos de Máquinas** para ver o catálogo de máquinas criado.

Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó **Catálogos de Máquinas**, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo.
2. Clique em **Criar Catálogo de Máquinas**. A página **Configuração do Catálogo de Máquinas** é exibida. Clique em **Avançar** nas páginas **Introdução**, **Tipo de Máquina** e **Gerenciamento de Máquinas**.
3. Na página **Imagem**:
   a. Selecione **Imagem preparada**.
   b. Em **Imagem preparada**, selecione uma versão de imagem de uma definição de imagem.
   c. Selecione a versão da imagem. Para ver mais detalhes sobre a versão da imagem selecionada, clique no número da versão, que está sublinhado.
4. Conclua as configurações nas páginas a seguir.
5. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.

Usar PowerShell

Criar uma imagem preparada

Os comandos detalhados do PowerShell para criar uma especificação de versão de imagem preparada são os seguintes:

1. Verifique os nomes de definição de imagem disponíveis usando o `Test-ProvImageDefinitionNameAvailable command`. Por exemplo,

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName xenimage1
   ```

2. Crie uma definição de imagem usando o comando `New-ProvImageDefinition`. Por exemplo,

   ```
   $ImageDefintion = New-ProvImageDefinition -ImageDefinitionName
   xenimage1 -OsType Windows -VdaSessionSupport SingleSession
   ```

3. Crie uma nova configuração para definição de imagem na conexão de hospedagem especificada usando o comando `Add-ProvImageDefinitionConnection`.

```
Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -HypervisorConnectionName
XenServer1
```

4. Crie uma versão de imagem usando o comando `New-ProvImageVersion`. Por exemplo,

```
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. Adicione uma especificação de versão de imagem mestre à versão da imagem usando o comando `Add-ProvImageVersionSpec`. Por exemplo,

```
$MasterImagePath = "XDHyp:\HostingUnits\xenhu \win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName xenhu
-MasterImagePath $MasterImagePath
```

> **Nota:**
>
> Você pode adicionar apenas uma especificação de versão de imagem mestre a uma versão de imagem para uma unidade de hospedagem.

6. Crie uma especificação de versão de imagem preparada a partir da especificação de versão de imagem mestre usando o comando `New-ProvImageVersionSpec`. Por exemplo,

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}

-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. Você também pode compartilhar a especificação de versão de imagem preparada com outra unidade de hospedagem dentro da mesma conexão de hospedagem usando o comando `Add-ProvImageVersionSpecHostingUnit`. Por exemplo,

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName xenhu2
```

Exemplo do conjunto completo de comandos Powershell para criar definição de imagem, versão de imagem e especificação de versão de imagem preparada:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName xenimage1
-OsType Windows -VdaSessionSupport SingleSession




Add-ProvImageDefinitionConnection -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -HypervisorConnectionName XenServer1



$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"



$MasterImagePath = "XDHyp:\HostingUnits\xenhu \win10-master.vm\win10-
master-snap.snapshot"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName xenhu -MasterImagePath
$MasterImagePath




New-ProvImageVersionSpec -SourceImageVersionSpecUid
```

```
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\xenhu\VM Network.network"}

 -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously



Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName xenhu2
```

Nota:

- Uma versão de imagem pode ter apenas uma especificação de versão de imagem mestre e uma especificação de versão de imagem preparada.
- Todas as especificações de versão de imagem devem ter um perfil de máquina ou nenhuma das especificações de versão de imagem deve ter um perfil de máquina.

Crie um catálogo usando uma especificação de versão de imagem preparada

Crie um catálogo de máquinas MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

Ou,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
```

```
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

Exemplo de criação de um catálogo usando uma especificação de versão de imagem preparada no XenServer:

```
New-ProvScheme -ProvisioningSchemeName assignimage -imageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid 1 `

  -HostingUnitName xenhu -IdentityPoolName poo1 `

  -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

  -NetworkMapping @{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}
```

Exemplo do conjunto completo de comandos Powershell para criar um catálogo:

```
$CatalogName = "XenCatalog"

$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" `

  -Name $CatalogName -PersistUserChanges "Discard" -ProvisioningType "MCS"
-Scope @() -SessionSupport "MultiSession"




$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "xen.local"
-IdentityPoolName $CatalogName `

  -IdentityType "ActiveDirectory"  -NamingScheme "xen##" -NamingSchemeType
"Numeric" -Scope @()
```

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
xenimage1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"




$Task = New-ProvScheme -ProvisioningSchemeName $CatalogName
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid `

  -HostingUnitName xenhu -IdentityPoolName $CatalogName -CleanOnBoot
-Scope @() -SecurityGroup @() `

  -NetworkMapping @{"0"="XDHyp:\HostingUnits\xenhu\VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName $CatalogName




Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Mais informações

- Gerenciamento de imagens

Onde ir em seguida

- Gerenciar catálogos criados usando imagens preparadas

Gerenciar catálogos criados usando imagens preparadas

Você pode atualizar um catálogo de máquinas MCS existente com uma imagem preparada diferente e gerenciar as definições e versões da imagem usando:

- Studio

- PowerShell

Usar o Studio

Atualizar um catálogo de máquinas com uma imagem preparada diferente

Para atualizar um catálogo de máquinas MCS existente com uma imagem preparada diferente, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel esquerdo e selecione um catálogo de máquinas que você deseja atualizar. Clique com o botão direito e selecione **Alterar Imagem Preparada**.
2. Na página **Imagem**, selecione uma imagem preparada. Se necessário, adicione uma nota para a imagem preparada selecionada.

   > **Nota:**
   >
   > (Somente Azure) Você também pode escolher uma imagem com ACG não habilitado e, posteriormente, selecionar a caixa de seleção **Colocar imagem preparada na Galeria de Computação do Azure** para colocar as imagens na galeria.

3. Para reverter para uma imagem preparada atribuída anteriormente, clique em **Usar atribuição de imagem anterior para reversão rápida** na parte inferior do assistente.

   Uma nova janela é aberta e exibe uma lista de todas as atribuições de imagem históricas disponíveis. Ao selecionar uma imagem da lista, a versão correspondente é selecionada automaticamente na árvore de imagens preparadas na página da imagem.
4. Na página **Estratégia de implantação**, selecione quando você deseja atualizar este catálogo com a imagem preparada selecionada.
5. Na página **Resumo**, verifique os detalhes. Clique em **Concluir**.

Para visualizar o histórico de alterações de imagem feitas em um catálogo, siga estas etapas:

1. Selecione um catálogo de máquinas.
2. Na guia **Template Properties**, no campo **Prepared image**, clique em **View Image history**.

Gerenciar as definições e versões de imagem

Você pode editar e excluir as definições e versões de imagem para gerenciar o uso de várias versões e definições de imagem criadas.

EDITAR UMA DEFINIÇÃO DE IMAGEM

Você pode editar o nome e a descrição de uma definição de imagem.

Para editar uma definição de imagem, faça o seguinte:

1. Vá para o nó **Images**, selecione uma definição de imagem e selecione **Edit Image Definition**.

EDITAR VERSÃO DA IMAGEM

Você pode editar a descrição de uma versão de imagem para especificar a finalidade dessa versão de imagem.

Para editar uma versão de imagem, faça o seguinte:

1. Vá para o nó **Images**, selecione uma versão de imagem e selecione **Edit Description**.

EXCLUIR UMA VERSÃO DE IMAGEM

Para excluir uma versão de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma versão de imagem e selecione **Excluir Versão da Imagem**.

> **Observação:**
>
> Você não pode excluir uma versão de imagem se ela for usada por um catálogo de máquinas.

EXCLUIR UMA DEFINIÇÃO DE IMAGEM

Para excluir uma definição de imagem, faça o seguinte:

1. Vá para o nó **Imagens**, selecione uma definição de imagem e selecione **Excluir Definição de Imagem**.

> **Observação:**
>
> Você não pode excluir uma definição de imagem se ela contiver uma versão de imagem.

Usar PowerShell

Atualizar um catálogo usando uma especificação de versão de imagem preparada

Você pode atualizar um catálogo usando o comando `Set-ProvSchemeImage`. Por exemplo,

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]

[-ImageAssignmentNote <string>]
```

Ou,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]

[-ImageAssignmentNote <string>]
```

Exemplo do conjunto completo de comandos do PowerShell para atualizar um catálogo:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"



Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously -ImageAssignmentNote "Update from VST team"
```

Obter o histórico de alterações da imagem para o esquema de provisionamento

```
Get-ProvSchemeImageVersionSpecHistory -ProvisioningSchemeName azurecatalog
```

Excluir definição de imagem, versão de imagem e especificação de versão de imagem preparada

Considere o seguinte antes de excluir uma definição de imagem, versão de imagem e especificação de versão de imagem preparada:

- Uma definição de imagem não pode ser excluída se contiver qualquer versão de imagem.

- Uma versão de imagem não pode ser excluída se contiver qualquer especificação de versão de imagem.
- Uma especificação de versão de imagem mestre não pode ser excluída se for usada por qualquer outra especificação de versão de imagem preparada.
- Uma especificação de versão de imagem preparada não pode ser excluída se for usada por qualquer catálogo de máquinas MCS.
- Uma unidade de hospedagem não pode ser excluída se for usada por qualquer outra especificação de versão de imagem preparada.

As etapas detalhadas são as seguintes:

1. Remova o catálogo de máquinas. Por exemplo,

```
Remove-ProvScheme -ProvisioningScheneName decouplingCatalog
```

2. Remova a especificação de versão de imagem preparada compartilhada. Por exemplo,

```
Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>
-HostingUnitName AzureWest
```

3. Remova uma especificação de versão de imagem preparada. Por exemplo,

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec
-ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
"PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

4. Remova a especificação de versão de imagem mestre. Por exemplo,

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"
```

```
Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronousl
```

Nota:

A especificação de versão de imagem mestre só pode ser excluída quando não houver nenhuma especificação de versão de imagem preparada associada.

5. Remova uma versão de imagem. Por exemplo,

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

6. Remova a configuração para a definição de imagem na conexão de hospedagem especificada. Por exemplo,

```
Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx
```

7. Remover uma definição de imagem. Por exemplo,

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

Exemplo do conjunto completo de comandos PowerShell quando a imagem preparada não é compartilhada entre unidades de host:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"


Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously


Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1


Remove-ProvImageDefinition -ImageDefinitionName image1
```

Exemplo do conjunto completo de comandos PowerShell quando a imagem preparada é compartilhada entre unidades de host:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog


Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>

-HostingUnitName AzureWest


$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"


Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously


$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
```

```
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1



Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx



Remove-ProvImageDefinition -ImageDefinitionName image1
```

Gerenciar definição de imagem e versão de imagem

Você pode renomear e editar uma definição de imagem, e editar uma versão de imagem.

- Renomear uma definição de imagem usando o comando `Rename-ProvImageDefinition`. Por exemplo:

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
  -NewImageDefinitionName <string>
  ```

  Ou,

  ```
  Rename-ProvImageDefinition -ImageDefinitionName <string>
  -NewImageDefinitionName <string>
  ```

- Editar uma definição de imagem usando o comando `Set-ProvImageDefinition`. Por exemplo:

  ```
  Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
  <string>]
  ```

Ou,

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
<string>]
```

- Editar uma versão de imagem usando o comando `Set-ProvImageVersion`. Por exemplo:

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
```

Ou,

```
Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
<int> [-Description <string>]
```

Obter detalhes da definição de imagem, versão da imagem, especificação da versão da imagem preparada e esquema de provisionamento

- Obter detalhes da definição de imagem usando o comando `Get-ProvImageDefinition`. Por exemplo:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- Obter detalhes da versão da imagem usando o comando `Get-ProvImageVersion`. Por exemplo:
  - Para listar as versões de imagem em uma definição de imagem,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    Ou,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - Para obter detalhes de uma versão de imagem,

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

Ou,

```
Get-ProvImageVersion -ImageDefinitionName <string>
-ImageVersionNumber <int>
```

- Obtenha a especificação da versão da imagem preparada usando o comando `Get-ProvImageVersionSpec`. Por exemplo:
  - Para listar todas as especificações de versão de imagem preparada em uma versão de imagem,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid>
    ```

  - Para listar as especificações da versão da imagem mestre em uma especificação de versão de imagem preparada,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
    'PreparationType -eq "None"'
    ```

  - Para listar as especificações da versão da imagem preparada em uma versão de imagem, que está associada a uma imagem mestre,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
    'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
    "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
    ```

  - Para obter especificações de versão de imagem preparada bem-sucedidas em uma versão de imagem,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
    'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
    "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
    -eq "Complete"'
    ```

  - Para obter detalhes de uma especificação de versão de imagem preparada,

    ```
    Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
    ```

- Obtenha os detalhes do esquema de provisionamento usando o comando `Get-ProvScheme`. Por exemplo:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
[-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
```

- Obtenha o histórico da especificação da versão da imagem preparada de um esquema de provisionamento usando o comando `Get-ProvSchemeImageVersionSpecHistory`. Por exemplo:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

Mais informações

- Gerenciamento de imagens

Criar catálogos de máquinas

Nota:

Este artigo descreve como criar catálogos usando o Studio. Se você estiver usando o Quick Deploy para criar recursos do Azure, siga as orientações em Criar catálogos usando o Quick Deploy.

Coleções de máquinas físicas ou virtuais são gerenciadas como uma única entidade chamada catálogo de máquinas. Dentro de um catálogo de máquinas, todas as máquinas compartilham um tipo de sistema operacional comum, que pode ser um SO multi-sessão ou um SO de sessão única, como sistemas baseados em Windows ou Linux.

Nota:

> Para obter mais informações sobre o provisionamento de máquinas macOS usando catálogos de máquinas, consulte este artigo na documentação do VDA para macOS.

> O Studio o guia para criar o primeiro catálogo de máquinas. Depois de criar o primeiro catálogo, você cria o primeiro grupo de entrega. Mais tarde, você pode alterar o catálogo que criou e criar mais catálogos.

Visão geral

Ao criar um catálogo de VMs, você especifica como provisionar essas VMs. Você pode usar o Machine Creation Services™ (MCS). Ou, você pode usar suas próprias ferramentas para fornecer máquinas.

- Se você usar o MCS para provisionar VMs, você fornece uma imagem (ou instantâneo) para criar VMs idênticas no catálogo. Antes de criar o catálogo, você deve configurar uma conexão de hospedagem pela primeira vez com o hipervisor ou serviço de nuvem de sua escolha e, em seguida, deve criar e configurar a imagem mestre no mesmo. A configuração da imagem mestre requer tarefas como ingresso no domínio quando necessário, instalação de drivers necessários, aplicativos a serem publicados e implantação do Virtual Delivery Agent (VDA) na imagem.
- Depois de criar a imagem mestre, você cria o catálogo de máquinas no Studio. Você seleciona essa imagem (ou um instantâneo de uma imagem), especifica o número de VMs a serem criadas no catálogo e configura informações adicionais.
- Se suas máquinas já estiverem disponíveis, você ainda deve criar um ou mais catálogos de máquinas para importar essas VMs para o catálogo.

Ao usar o MCS para criar o primeiro catálogo, você especifica uma unidade de hospedagem que você criou anteriormente. A unidade de hospedagem fornece configuração de recursos para você criar uma máquina virtual. Mais tarde (depois de criar seu primeiro catálogo e grupo de entrega), você pode alterar informações sobre essa unidade de hospedagem ou sua conexão de host pai ou criar mais conexões e unidades de hospedagem.

Se um Cloud Connector não estiver operando corretamente, as operações de provisionamento do MCS (como atualizações de catálogo) demoram mais do que o normal, e o desempenho da interface de gerenciamento degrada-se significativamente.

Verificação de licença RDS

A criação de um catálogo de máquinas contendo máquinas de SO multi-sessão Windows inclui uma verificação automática de licenças RDS da Microsoft válidas. O catálogo é pesquisado por uma máquina ligada e registrada para realizar a verificação.

- Se uma máquina ligada e registrada não puder ser encontrada, um aviso será exibido, explicando que a verificação de licenciamento RDS não pode ser realizada.
- Se uma máquina for encontrada e um erro for detectado, o Studio exibirá uma mensagem de aviso para o catálogo contendo o problema detectado. Para remover um aviso de licença RDS de um catálogo (para que ele não apareça mais na exibição), selecione o catálogo. Selecione **Remover aviso de licença RDS**. Quando solicitado, confirme a ação.

Registro de VDA

Um VDA deve ser registrado em um Cloud Connector para ser considerado ao iniciar sessões intermediadas. VDAs não registrados podem resultar na subutilização de recursos que, de outra forma, estariam disponíveis. Existem várias razões pelas quais um VDA pode não estar registrado, muitas das quais você pode solucionar. As informações de solução de problemas são fornecidas no assistente de criação de catálogo e depois que você adiciona um catálogo a um grupo de entrega.

No assistente de criação de catálogo, depois de adicionar máquinas existentes, a lista de nomes de contas de computador indica se cada máquina é adequada para ser adicionada ao catálogo. Passe o mouse sobre o ícone ao lado de cada máquina para exibir uma mensagem informativa sobre ela.

Se a mensagem identificar uma máquina problemática, você pode remover essa máquina (usando o botão **Remover**) ou adicionar a máquina. Por exemplo, se uma mensagem indicar que as informações não podem ser obtidas sobre uma máquina (talvez porque nunca foi registrada), você pode optar por adicionar a máquina de qualquer maneira.

Para obter mais informações sobre a solução de problemas de registro de VDA, consulte CTX136668.

Resumo da criação de catálogo MCS

Aqui está uma breve visão geral das ações padrão do MCS depois que você fornece informações no assistente de criação de catálogo.

- Se você selecionar uma imagem (em vez de um snapshot), o MCS criará um snapshot.

- O MCS cria uma cópia completa do snapshot e a coloca em cada local de armazenamento definido na conexão do host.
- O MCS adiciona as máquinas ao Active Directory, o que cria identidades exclusivas.
- O MCS cria o número de VMs especificado no assistente, com dois discos definidos para cada VM. Além dos dois discos por VM, uma cópia completa do snapshot ou da imagem mestre também é armazenada no mesmo local de armazenamento. Se você tiver vários locais de armazenamento definidos, cada um receberá os seguintes tipos de disco:
  - A cópia completa do snapshot (mencionada anteriormente), que é somente leitura e compartilhada entre as VMs recém-criadas.
  - Um disco de identidade exclusivo de 16 MB que dá a cada VM uma identidade única. Cada VM recebe um disco de identidade.
  - Um disco de diferença exclusivo para armazenar gravações feitas na VM. Este disco é provisionado de forma fina (se suportado pelo armazenamento do host) e aumenta para o tamanho máximo da imagem mestre, se necessário. Cada VM recebe um disco de diferença. O disco de diferença mantém as alterações feitas durante as sessões. É permanente para desktops dedicados. Para desktops agrupados, ele é excluído e um novo é criado após cada reinício.
- Para VMs Windows na versão VDA 2511 (Atualização 1) ou posterior, o MCS pode atribuir um `MachineGuid` exclusivo a cada máquina. Este `MachineGuid` é usado para fins de licenciamento por alguns softwares instalados no VDA. Este comportamento é desativado por padrão, mas pode ser ativado definindo o valor da chave de registro `HKLM:\Software\Citrix\MachineIdentityServiceAgent\EnableUniqueMachineGuid` como `1` na imagem mestre ou em máquinas individuais.

Alternativamente, ao criar VMs para entregar desktops estáticos, você pode especificar (na página **Máquinas** do assistente de criação de catálogo) clones de VM espessos (cópia completa). Clones completos não exigem a retenção da imagem mestre em cada armazenamento de dados. Cada VM tem seu próprio arquivo.

Considerações de armazenamento do MCS

Existem muitos fatores ao decidir sobre soluções de armazenamento, configurações e capacidades para o MCS. As informações a seguir fornecem considerações adequadas para a capacidade de armazenamento:

Considerações de capacidade:

- Discos

  Os discos Delta ou de Diferença (Diff) consomem a maior quantidade de espaço na maioria das implantações do MCS para cada VM. Cada VM criada pelo MCS recebe no mínimo 2 discos na criação.

  - Disk0 = Disco Diff: contém o SO quando copiado da imagem mestre base.
  - Disk1 = Disco de Identidade: 16 MB - contém dados do Active Directory para cada VM.

  À medida que o produto evolui, pode ser necessário adicionar mais discos para satisfazer certos casos de uso e consumo de recursos. Por exemplo:

  - Otimização de Armazenamento do MCS cria um disco estilo cache de gravação para cada VM. Em ambientes de virtualização XenServer, VMware e SCVMM, o MCS coloca o disco de cache de gravação (WBC) no mesmo local de armazenamento que o disco do SO se você configurar a lista de armazenamento de SO disponível da mesma forma que a lista de armazenamento temporário disponível ao criar uma conexão de host.
  - O MCS adicionou a capacidade de usar clones completos em oposição ao cenário de disco Delta descrito na seção anterior.

  Recursos do hipervisor também podem entrar na equação. Por exemplo:

  - XenServer IntelliCache cria um Disco de Leitura no armazenamento local para cada XenServer. Esta opção economiza IOPS contra a imagem que pode estar localizada no local de armazenamento compartilhado.

- Sobrecarga do hypervisor

  Diferentes hypervisors usam arquivos específicos que criam sobrecarga para VMs. Os hypervisors também usam armazenamento para gerenciamento e operações gerais de registro. Calcule o espaço para incluir a sobrecarga para:

  - Arquivos de log
  - Arquivos específicos do hypervisor. Por exemplo:
    - O VMware adiciona mais arquivos à pasta **VM storage**. Consulte Melhores Práticas do VMware.
    - Calcule os requisitos totais de tamanho da sua máquina virtual. Considere uma máquina virtual contendo 20 GB para o disco virtual, 16 GB para o arquivo de troca e 100 MB para arquivos de log, consumindo um total de 36,1 GB.

    - Snapshots para XenServer; Snapshots para VMware.

- Sobrecarga de processo

  A criação de um catálogo, a adição de uma máquina e a atualização de um catálogo têm implicações de armazenamento únicas. Por exemplo:

    - Criação inicial do catálogo requer que uma cópia do disco base seja copiada para cada local de armazenamento.
    - Adicionar uma máquina a um catálogo não requer a cópia do disco base para cada local de armazenamento. A criação do catálogo varia com base nos recursos selecionados.
    - Atualizar o catálogo para criar um disco base extra em cada local de armazenamento. As atualizações do catálogo também experimentam um pico temporário de armazenamento onde cada VM no catálogo tem 2 discos Diff por um certo período de tempo.

Mais considerações:

- **Dimensionamento da RAM:** Afeta o tamanho de certos arquivos e discos do hypervisor, incluindo discos de otimização de E/S, cache de gravação e arquivos de snapshot.
- **Thin / Thick provisioning:** O armazenamento NFS é preferido devido aos recursos de provisionamento thin.

Otimização de armazenamento do Machine Creation Services (MCS)

O recurso de otimização de armazenamento do Machine Creation Services (MCS) também é conhecido como MCS I/O. Esse recurso está disponível apenas no Azure, GCP, XenServer, VMware, AWS e SCVMM.

- O contêiner de cache de gravação é *baseado em arquivo*, a mesma funcionalidade encontrada no Citrix Provisioning. Por exemplo, o nome do arquivo de cache de gravação do Citrix Provisioning é `D:\vdiskdif.vhdx` e o nome do arquivo de cache de gravação do MCS I/O é `D:\mcsdif.vhdx`.
- Obtenha melhorias de diagnóstico incluindo suporte para um arquivo de despejo de memória do Windows gravado no disco de cache de gravação.
- O MCS I/O mantém a tecnologia *cache na RAM com estouro para o disco rígido* para fornecer a solução de cache de gravação de várias camadas mais otimizada. Essa funcionalidade permite que um administrador equilibre o custo em cada camada, RAM e disco, e o desempenho para atender à expectativa de carga de trabalho desejada.

A atualização do método de cache de gravação de *baseado em disco* para *baseado em arquivo* requer as seguintes alterações:

1. O MCS I/O não oferece mais suporte a cache somente RAM. Especifique um tamanho de disco durante a criação do catálogo de máquinas.
2. O disco de cache de gravação da VM é criado e formatado automaticamente ao inicializar uma VM pela primeira vez. Assim que a VM estiver ativa, o arquivo de cache de gravação `mcsdif.vhdx` é gravado no volume formatado `MCSWCDisk`.
3. O arquivo de paginação é redirecionado para este volume formatado, `MCSWCDisk`. Como resultado, esse tamanho de disco considera a quantidade total de espaço em disco. Ele inclui o delta entre o tamanho do disco e a carga de trabalho gerada mais o tamanho do arquivo de paginação. Isso geralmente está associado ao tamanho da RAM da VM.

Habilitar atualizações de otimização de armazenamento do MCS

Para habilitar o recurso de otimização de armazenamento MCS I/O, atualize o Cloud Connector e o VDA para a versão mais recente do Citrix DaaS.

> **Nota:**
>
> Se você atualizar uma implantação existente que tenha o MCS I/O habilitado, nenhuma configuração adicional será necessária. A atualização do VDA e do Delivery Controller manipular a atualização do MCS I/O.

> Para obter informações sobre como atribuir uma letra de unidade ao disco de cache de write-back, consulte Atribuir uma letra de unidade específica ao disco de cache de write-back do MCS I/O.

Prepare uma imagem mestre no hipervisor ou serviço de nuvem

A imagem mestre contém o sistema operacional, aplicativos não virtualizados, VDA e outros softwares.

Bom saber:

- Uma imagem mestre também pode ser conhecida como imagem de clone, imagem dourada, VM base ou imagem base. Fornecedores de host e provedores de serviços de nuvem podem usar termos diferentes.

- Certifique-se de que o hipervisor ou serviço de nuvem tenha processadores, memória e armazenamento suficientes para acomodar o número de máquinas criadas.
- Configure a quantidade correta de espaço em disco rígido necessário para desktops e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo de máquinas.
- Os catálogos de máquinas do Acesso Remoto para PC não usam imagens mestre.
- Considerações sobre a ativação do Microsoft KMS ao usar o MCS: Se sua implantação incluir VDAs 7.x com um host XenServer 6.1 ou 6.2, vSphere ou Microsoft System Center Virtual Machine Manager, você não precisará rearmar manualmente o Microsoft Windows ou o Microsoft Office.

Instale e configure o seguinte software na imagem mestre:

- Ferramentas de integração para seu hipervisor (como Citrix VM Tools, Hyper-V Integration Services ou VMware tools). Se você omitir esta etapa, os aplicativos e desktops podem não funcionar corretamente.
- Um VDA. A Citrix recomenda instalar a versão mais recente do VDA para permitir o acesso aos recursos mais recentes. A falha na instalação de um VDA na imagem mestre faz com que a criação do catálogo falhe.
- Ferramentas de terceiros conforme necessário, como software antivírus ou agentes de distribuição eletrônica de software. Configure os serviços com configurações apropriadas para os usuários e o tipo de máquina (como recursos de atualização).
- Aplicativos de terceiros que você não está virtualizando. A Citrix recomenda virtualizar aplicativos. A virtualização reduz custos, eliminando a necessidade de atualizar a imagem mestre após adicionar ou reconfigurar um aplicativo. Além disso, menos aplicativos instalados reduzem o tamanho dos discos rígidos da imagem mestre, o que economiza custos de armazenamento.
- Clientes App-V com as configurações recomendadas, se você planeja publicar aplicativos App-V. O cliente App-V está disponível na Microsoft.
- Ao usar o MCS, se você localizar o Microsoft Windows, instale as localidades e os pacotes de idiomas. Durante o provisionamento, quando um instantâneo é criado, as VMs provisionadas usam as localidades e os pacotes de idiomas instalados.

> **Importante:**

> Se você estiver usando o MCS, não execute o Sysprep em imagens mestre.

> Para preparar uma imagem mestre:

1. Usando a ferramenta de gerenciamento do seu hipervisor, crie uma imagem mestre e, em seguida, instale o sistema operacional e todos os service packs e atualizações. Especifique o número de vCPUs. Você também pode especificar o valor da vCPU se criar o catálogo de máquinas usando o PowerShell. Você não pode especificar o número de vCPUs ao criar um catálogo no Studio. Configure a quantidade de espaço em disco rígido necessária para desktops e aplicativos. Esse valor não pode ser alterado posteriormente ou no catálogo.
2. Certifique-se de que o disco rígido esteja conectado no local do dispositivo 0. A maioria dos modelos de imagem mestre padrão configura este local por padrão, mas alguns modelos personalizados podem não fazê-lo.
3. Instale e configure o software listado acima na imagem mestre.
4. Se você não estiver usando o MCS, junte a imagem mestre ao domínio do qual os aplicativos e desktops são membros. Certifique-se de que a imagem mestre esteja disponível no host onde as máquinas são criadas. Se você estiver usando o MCS, não é necessário unir a imagem mestre a um domínio. As máquinas provisionadas são unidas ao domínio especificado no assistente de criação de catálogo.
5. A Citrix recomenda que você crie e nomeie um instantâneo de sua imagem mestre para que possa ser identificado posteriormente. Se você especificar uma imagem mestre em vez de um instantâneo ao criar um catálogo, a interface de gerenciamento criará um instantâneo, mas você não poderá nomeá-lo.

Ativação de licenciamento por volume

O MCS oferece suporte à ativação de licenciamento por volume para automatizar e gerenciar a ativação de sistemas operacionais Windows e Microsoft Office. Os três modelos que o MCS oferece suporte para ativação de licenciamento por volume são:

- Serviço de Gerenciamento de Chaves (KMS)
- Ativação baseada no Active Directory (ADBA)
- Chave de Ativação Múltipla (MAK)

Você pode alterar a configuração de ativação depois de criar o catálogo de máquinas.

Serviço de Gerenciamento de Chaves (KMS)

O KMS é um serviço leve que não requer um sistema dedicado e pode ser facilmente co-hospedado em um sistema que fornece outros serviços. Essa funcionalidade é suportada em todas as versões do Windows compatíveis com Citrix. Durante a preparação da imagem, o MCS

faz o rearmamento do KMS do Microsoft Windows e do Microsoft Office. Você pode pular o rearmamento executando o comando `Set-Provserviceconfigurationdata`. Para obter mais informações sobre a ativação do KMS, consulte Ativar usando o Serviço de Gerenciamento de Chaves.

> **Nota:**
>
> Todos os catálogos de máquinas criados após a execução do comando `Set-Provserviceconfigurationdata` têm a mesma configuração fornecida no comando.

Ativação baseada no Active Directory (ADBA)

O ADBA permite ativar máquinas por meio de suas conexões de domínio. As máquinas são ativadas imediatamente quando ingressam no domínio. Essas máquinas permanecem ativadas enquanto permanecerem ingressadas no domínio e em contato com ele. Essa funcionalidade é suportada em todas as versões do Windows compatíveis com Citrix. Para obter mais informações sobre a ativação baseada no Active Directory, consulte Ativar usando ativação baseada no Active Directory.

Chave de Ativação Múltipla (MAK)

MAK é uma forma de ativar o volume e autenticar o sistema Windows com a ajuda do servidor Microsoft. Você deve comprar a chave MAK da Microsoft, que é atribuída a um número fixo de contagens de ativação. Cada vez que um sistema Windows é ativado, a contagem de ativação é reduzida. Existem duas maneiras de ativar o sistema:

- Ativação Online: Se o sistema Windows que você deseja ativar tiver acesso à internet, o sistema ativa automaticamente o Windows ao instalar a chave do produto. Esse processo reduz a contagem de ativação em 1 para o MAK correspondente.
- Ativação Offline: Se o sistema Windows não conseguir se conectar à internet para fazer a ativação online, o MCS obtém um ID de confirmação e um ID de instalação do servidor Microsoft para ativar o sistema Windows. Essa forma de ativação é útil para catálogos de máquinas não persistentes.

> **Nota:**
>
> - O MCS não oferece suporte à ativação do Microsoft Office usando MAK.

- A versão mínima do VDA necessária é 2303.

Requisitos principais

- O Delivery Controller™ deve ter acesso à internet.
- Crie um novo catálogo se a nova imagem a ser atualizada tiver uma Chave MAK diferente da original.
- Instale a chave MAK na imagem mestre. Consulte Implantar Ativação MAK para obter as etapas para instalar a Chave MAK em um Sistema Windows.
- Se você não estiver usando a preparação de imagem:

  a. Adicione o valor DWORD do registro `Manual` em `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`.

  b. Defina o valor como `1`.

Contagens de Ativação

Para visualizar o número de ativações restantes para a Chave MAK ou para verificar se uma VM está consumindo duas ou mais ativações, use a Ferramenta de Gerenciamento de Ativação de Volume (VAMT). Consulte Instalar VAMT.

Ativar o sistema Windows usando MAK

Para ativar o sistema Windows usando MAK:

1. Instale a chave do produto na imagem mestre. Esta etapa consome uma contagem de ativação.
2. Crie um catálogo de máquinas MCS.
3. Se você não estiver usando a preparação de imagem:

   a. Adicione o valor DWORD do registro `Manual` em `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`.

   b. Defina o valor como `1`.

   Este método desabilita a opção de ativação online.
4. Adicione VMs ao catálogo de máquinas.
5. Ligar as VMs.

6. Dependendo se é ativação online ou offline, o sistema Windows é ativado.
    - Se a ativação for online, o sistema Windows é ativado após a instalação da chave do produto.
    - Se a ativação for offline, o MCS se comunica com as VMs provisionadas para obter o status de ativação do sistema Windows. O MCS então recupera um ID de confirmação e um ID de instalação do servidor Microsoft. Esses IDs são usados para ativar o sistema Windows.

Solução de problemas

Se a VM provisionada não for ativada com a chave MAK instalada, execute o comando `Get-ProvVM` ou `Get-ProvScheme` em uma janela do PowerShell.

- O comando `Get-ProvScheme`: Consulte o parâmetro `WindowsActivationType` associado ao catálogo de máquinas MCS da imagem mestre mais recente.
- O comando `Get-ProvVM`. Consulte os parâmetros `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorCode` e `WindowsActivationStatusError`.

Você pode verificar o erro e as etapas para resolver o problema.

Criar um catálogo de máquinas usando o Studio

Antes de criar um catálogo:

- Certifique-se de ter criado uma conexão com o hipervisor, serviço de nuvem ou outro recurso que hospeda suas máquinas.
- Se você criou uma imagem mestre para provisionar máquinas. Certifique-se de ter instalado um VDA nessa imagem mestre.

> **Nota:**
>
> Ao usar um serviço de nuvem ou hipervisor para hospedar VMs, o assistente de criação de catálogo pode conter páginas extras específicas para esse host. Por exemplo, ao usar uma imagem mestre do Azure Resource Manager, o assistente de criação de catálogo contém uma página **Tipos de Armazenamento e Licença**. Para obter informações específicas do host, consulte os artigos específicos mencionados em Onde ir em seguida.

Iniciar o assistente de criação de catálogo

1. Faça login em Citrix Cloud.
2. No bloco **DaaS**, clique em **Gerenciar** para abrir o Studio.
3. Selecione **Catálogos de Máquinas** no painel esquerdo.
4. Se este for o primeiro catálogo a ser criado, você será guiado para a seleção correta (como "Configurar as máquinas e criar catálogos de máquinas para executar aplicativos e desktops"). O assistente de criação de catálogo é aberto.
5. Se você já criou um catálogo e deseja criar outro, siga estas etapas:

    a. Para organizar catálogos usando pastas, crie pastas sob a pasta padrão **Catálogos de Máquinas**. Para obter mais informações, consulte Criar uma pasta de catálogo.

    b. Selecione a pasta onde você deseja criar o catálogo e clique em **Criar Catálogo de Máquinas**. O assistente de criação de catálogo é aberto.

O assistente o guiará pelas páginas descritas nas seções a seguir. As páginas que você vê podem diferir, dependendo das seleções que você faz e da conexão (com um host) que você usa. Hosts / recursos de virtualização lista as fontes de informação para os tipos de host suportados.

Selecionar um tipo de máquina

Cada catálogo deve conter máquinas de apenas um tipo de SO. Selecione uma das seguintes opções na página **Tipo de Máquina**:

- **SO multissessão:** Um catálogo de SO multissessão fornece desktops compartilhados hospedados. As máquinas podem estar executando versões compatíveis dos sistemas operacionais Windows ou Linux, mas o catálogo não pode conter sistemas operacionais Windows e Linux.
- **SO de sessão única:** Um catálogo de SO de sessão única fornece desktops VDI que você pode atribuir a diferentes usuários.
- **Acesso Remoto a PC:** Um catálogo de Acesso Remoto a PC fornece aos usuários acesso remoto às suas máquinas de desktop físicas do escritório. O Acesso Remoto a PC não requer uma VPN para fornecer segurança.

Selecionar opções de gerenciamento de máquina

> **Observação:**

> A página **Gerenciamento de Máquinas** não aparece se você selecionar **Acesso Remoto para PC** na página **Tipo de Máquina**.

> A página **Gerenciamento de Máquinas** indica como as máquinas são gerenciadas e a ferramenta que você deseja usar para implantar máquinas.

Selecione uma das opções para indicar como as máquinas devem ser gerenciadas em termos de energia:

- **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade)**: Esta opção está disponível apenas se você já configurou uma conexão para um hipervisor ou serviço de nuvem.
- **Máquinas sem gerenciamento de energia (por exemplo, máquinas físicas)**

Se você selecionar a opção **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade)**, então selecione uma ferramenta para criar VMs:

- **Citrix Provisioning™ Technology**
  - **Citrix Machine Creation Services (MCS)** Cria um catálogo de VMs provisionadas e com imagem usando o MCS. O MCS copia imagens clonadas de uma imagem mestre para essas VMs.
  - **Citrix Provisioning Services (PVS)** Cria um catálogo de VMs provisionadas usando o MCS e com imagem usando o PVS. Essas VMs servem como dispositivos de destino PVS e o servidor PVS pode transmitir uma única imagem de disco compartilhada para elas.

    > **Observação:**
    >
    > - Esta opção está disponível apenas para sites PVS registrados com o Citrix Cloud™ e está atualmente limitada a recursos do Azure.
    > - Ao criar um catálogo do Citrix Provisioning na página **Dispositivo de Destino**, você pode ver que no menu suspenso para selecionar a farm e o site para as máquinas a serem provisionadas, há farms e sites listados que não existem mais. Como solução alternativa, você pode executar o comando PowerShell `Unregister-HypPvsSite` para remover as farms e os sites do banco de dados. Para obter informações sobre o comando PowerShell, consulte Unregister-HypPvsSite.

- **Outro serviço ou tecnologia** Uma ferramenta que gerencia máquinas já existentes no data center. A Citrix recomenda que você use o Microsoft System Center Configuration Manager ou outro aplicativo de terceiros para garantir que as máquinas no catálogo sejam consistentes.

Observação:

Para máquinas com SO Linux, consulte Criar VDAs Linux usando Machine Creation Services (MCS).

Selecionar uma experiência de desktop

Nota:

As opções na página **Experiência de Desktop** variam de acordo com o tipo de máquina que você seleciona na página **Tipo de Máquina**.

- Para máquinas com **SO multissessão**, os usuários recebem um desktop aleatório cada vez que fazem login. Você tem as seguintes opções na página **Experiência de Desktop**:
  - Salvar alterações no disco local da máquina que hospeda desktops virtuais: Persistente
  - Descartar todas as alterações e limpar desktops virtuais quando o usuário faz logoff: Não persistente

  Nota:

  Para máquinas multissessão persistentes, as alterações que os usuários fazem nos desktops serão salvas e acessíveis a todos os usuários autorizados.

- Para máquinas com SO de sessão única, você tem as seguintes opções na página **Experiência de Desktop**:
  - Conectar a um novo desktop (aleatório) cada vez que os usuários fazem login.
  - Conectar ao mesmo desktop (estático) cada vez que os usuários fazem login.

Você pode decidir ainda se as alterações feitas pelos usuários serão salvas ou descartadas após o logoff.

Se você selecionar **Salvar alterações no disco local da máquina que hospeda desktops virtuais: Persistente**, as opções Fast Copy Clone ou Full Copy Clone estarão disponíveis para o modo **Cópia de máquina virtual** na página **Máquinas Virtuais**. Caso contrário, o modo **Cópia de máquina virtual** estará indisponível.

Selecionar uma imagem e um perfil de máquina

> **Nota:**
>
> - Esta página aparece somente se você selecionar **Citrix Machine Creation Services (MCS)** na página **Gerenciamento de Máquinas**.
> - As opções disponíveis nesta página variam de acordo com o hipervisor ou serviço de nuvem.

Siga estas etapas para concluir as configurações na página:

1. Selecione um tipo de imagem para o catálogo de máquinas e, em seguida, selecione uma imagem. Dois tipos de imagens estão disponíveis:

   - **Imagem mestre**: Um snapshot ou VM criado como a imagem mestre. Ele passa por preparação automática de imagem no início da criação do catálogo. Se necessário, você pode adicionar uma nota para a imagem selecionada.

     > **Nota:**
     >
     > - Ao usar o MCS, não execute o Sysprep em imagens mestre.
     > - Se você especificar uma imagem mestre em vez de um snapshot, a interface de gerenciamento criará um snapshot, mas você não poderá nomeá-lo.
     > - Uma mensagem de erro aparece se você selecionar um snapshot ou VM que não seja compatível com a tecnologia de gerenciamento de máquinas selecionada anteriormente no assistente.

- Para atualizar imagens dentro de um nó de imagem, selecione-o na árvore e clique na opção **Atualizar** no canto superior direito. Se você não selecionar nenhum nó de imagem, clicar em **Atualizar** atualiza todas as imagens na árvore. Para desmarcar um nó selecionado na árvore, mantenha **CTRL** pressionado e clique no nó.

- **Imagem preparada**: Uma imagem que passou por preparação de imagem, pronta para uso direto na criação de VM. Optar por imagens preparadas em vez de imagens mestre para a criação de catálogo garante uma criação de catálogo de máquinas mais rápida e confiável, juntamente com um gerenciamento simplificado do ciclo de vida da imagem. Se necessário, adicione uma nota para a imagem preparada selecionada.

  Nota:

  - VMs criadas usando imagens preparadas não suportam hibernação.
  - Atualmente, a criação de catálogos usando imagens preparadas está disponível apenas em ambientes Amazon WorkSpaces Core, Azure e VMware.
  - Imagens preparadas são necessárias para criar catálogos em ambientes Amazon WorkSpaces Core.

  Para obter mais informações sobre como criar imagens preparadas, consulte Gerenciamento de imagens.

2. Para herdar as configurações da VM de um perfil de máquina, selecione **Usar um perfil de máquina** e, em seguida, selecione uma VM ou especificação de modelo ARM (específica do Azure) para usar como perfil de máquina.

   Nota:

   - Atualmente, o uso de perfis de máquina é restrito a VMs do Azure, Amazon WorkSpaces Core, AWS, GCP e VMware.
   - Um perfil de máquina é necessário para criar catálogos em ambientes Amazon WorkSpaces Core.

3. Para implantações VMware, ao criar um catálogo de máquinas usando um perfil de máquina, você deve especificar a pasta onde deseja manter as máquinas virtuais.

Para fornecer o local da pasta da máquina virtual, no assistente de criação de catálogo, vá para a página **Máquinas Virtuais** e vá para a seção **Selecionar uma pasta para colocar as máquinas** e forneça o local da pasta da máquina virtual. Se não for especificado, o sistema considera a pasta do perfil de máquina selecionado como o local padrão.

1. Para implantações AWS, você pode selecionar um modelo de inicialização como perfil de máquina.
2. Selecione o nível funcional mínimo para o catálogo. Para habilitar o uso dos recursos mais recentes do produto, certifique-se de que a imagem mestre tenha a versão mais recente do VDA instalada.

Configurar as máquinas

> **Nota:**
>
> - O título desta página depende do que você selecionou na página **Gerenciamento de Máquinas**: **Máquinas**, **Máquinas Virtuais** ou **Máquinas e Usuários**.
> - Esta página não aparece se você selecionar **Acesso Remoto ao PC** na página **Tipo de Máquina**.
> - Você pode criar um catálogo vazio, o que significa que o catálogo não contém máquinas.

- **Ao usar o MCS para criar máquinas:**
  - Especifique quantas máquinas virtuais devem ser criadas. Digite **0** (zero) se não quiser criar nenhuma. Mais tarde, para criar VMs para um catálogo vazio, você pode executar **Adicionar máquinas**.
  - Escolha a quantidade de memória (em MB) que cada VM terá.

    > **Importante:**
    >
    > Cada VM criada tem um disco rígido. Seu tamanho é definido na imagem mestre; você não pode alterar o tamanho do disco rígido no catálogo.

- Se você indicar na página **Experiência da Área de Trabalho** que as alterações do usuário em áreas de trabalho estáticas devem ser salvas em um Personal vDisk separado, especifique o tamanho do disco virtual em GB e a letra da unidade.
- Se sua implantação usar mais de uma zona (local de recurso), você poderá selecionar uma zona para o catálogo.
- Se você estiver criando VMs de área de trabalho estáticas, selecione um modo de cópia de máquina virtual. Consulte Modo de cópia de máquina virtual.
- Se você estiver criando VMs de área de trabalho aleatórias não persistentes, poderá habilitar e configurar o cache de write-back para dados temporários nas máquinas para melhorar o desempenho de E/S. Para obter mais informações, consulte Configurar cache para dados temporários.

- **Ao usar outras ferramentas para fornecer máquinas:**

  Adicione (ou importe uma lista de) nomes de contas de máquina. Você pode alterar o nome da conta de uma VM depois de adicioná-la ou importá-la. Se você especificou máquinas estáticas na página **Experiência da Área de Trabalho**, pode, opcionalmente, especificar o nome de usuário para uso com cada VM que adicionar.

  > **Dica:**
  >
  > Para adicionar usuários, você pode navegar até os usuários ou inserir uma lista de nomes de usuário separados por ponto e vírgula manualmente. Se os usuários estiverem no Active Directory, insira os nomes diretamente. Caso contrário, insira os nomes neste formato: `<identity provider>:<user name>`. Exemplo: `AzureAD:username`.
  >
  > Depois de adicionar ou importar nomes, você pode usar o botão **Remover** para excluir nomes da lista enquanto ainda estiver nesta página do assistente.

- **Ao usar outras ferramentas (não MCS):**

  Um ícone e uma dica de ferramenta para cada máquina adicionada (ou importada) ajudam a identificar máquinas que podem não ser elegíveis para adicionar ao catálogo ou que não conseguem se registrar em um Cloud Connector.

Modo de cópia da máquina virtual

O modo de cópia que você especifica na página **Máquinas** determina se o MCS cria clones finos (cópia rápida) ou espessos (cópia completa) a partir da imagem mestre. (Padrão = clones finos)

- Use clones de cópia rápida para um uso de armazenamento mais eficiente e criação de máquina mais rápida.
- Use clones de cópia completa para melhor recuperação de dados e suporte à migração, com IOPS potencialmente reduzidos após a criação das máquinas.

> **Nota:**
>
> A abordagem de Clone de Cópia Completa está disponível apenas para provisionamento de VMs persistentes em sistemas operacionais de sessão única ou múltipla.

Configurar cache para dados temporários

Ao usar o MCS para gerenciar máquinas aleatórias não persistentes em um catálogo, você pode habilitar o cache de write-back para as máquinas para melhorar o desempenho de E/S.

O cache de write-back é conhecido como MCSIO. Para obter mais informações, consulte este artigo do blog.

PRÉ-REQUISITOS

Para habilitar o cache de write-back, o catálogo deve atender a estes requisitos:

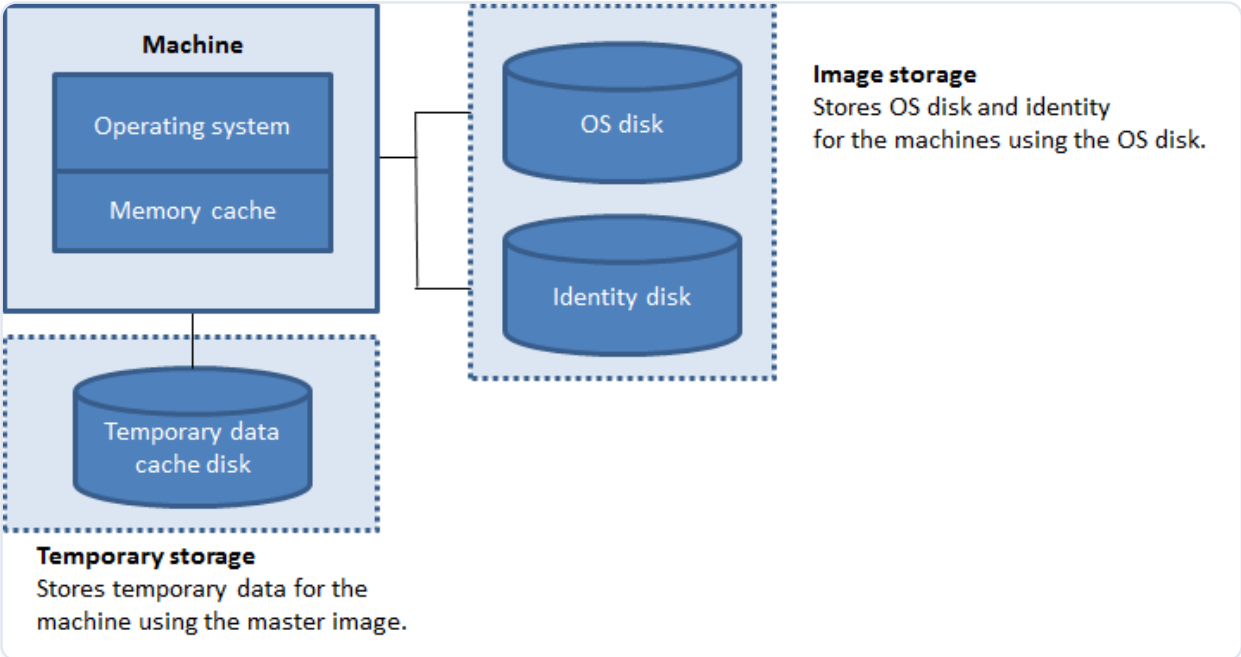
- Usa uma conexão que especifica o armazenamento para dados temporários. Para obter mais informações, consulte Conexões e recursos.
- Os VDAs devem ser pelo menos da versão 7.9 e instalados com um driver MCSIO atual.

  > **Nota:**
  >
  > Você pode instalar este driver ao instalar ou atualizar um VDA. Por padrão, esse driver não é instalado.

- Para habilitar a atribuição de letra de unidade para caches de disco, as VMs devem atender aos seguintes requisitos adicionais:
  - Sistema Operacional: Windows
  - Versão do VDA: 2305 ou posterior

CONSIDERAÇÕES

- Os caches de write-back vêm em cache de *Memória* e cache de *Disco*. Por padrão, seus valores padrão diferem de acordo com o tipo de conexão. Geralmente, os valores padrão são suficientes para a maioria dos casos; no entanto, considere o espaço necessário para:
  - Arquivos de dados temporários criados pelo próprio Windows, incluindo o arquivo de paginação do Windows.
  - Dados de perfil de usuário.
  - Dados do ShareFile que são sincronizados com as sessões dos usuários.
  - Dados que podem ser criados ou copiados por um usuário da sessão ou quaisquer aplicativos que os usuários possam instalar dentro da sessão.



- Ao habilitar o cache de write-back para dados temporários, use um cache de memória e um cache de disco. Os dados temporários são gravados primeiro no cache de memória. Quando o cache de memória atinge o limite configurado, os dados mais antigos são movidos para o cache de disco. **Nota:** O cache de write-back usando apenas um cache de disco não é mais suportado.
- O cache de memória faz parte da quantidade total de memória em cada máquina. Considere aumentar a quantidade total de memória em cada máquina após habilitar o cache de write-back.
- Alterar o **Tamanho do cache de disco (GB)** de seu valor padrão pode afetar o desempenho. O tamanho deve corresponder aos requisitos do usuário e à carga colocada na máquina.

> **Importante:**
>
> Se o cache de disco ficar sem espaço, a sessão do usuário se torna inutilizável.

- Se você desmarcar a caixa de seleção **Tamanho do cache de disco**, nenhum disco de cache é criado. Nesse caso, especifique um valor de **Memória alocada para cache** que seja grande o suficiente para armazenar todos os dados temporários. Isso é viável apenas se grandes quantidades de RAM estiverem disponíveis para alocação a cada VM.
- Não habilite o cache se você pretende usar este catálogo para criar AppDisks.
- Você não pode alterar os valores de cache em um catálogo de máquinas depois que ele é criado.

Usando arquivos CSV para adicionar máquinas em massa

Se você usa o Studio, pode adicionar máquinas em massa usando arquivos CSV. O recurso está disponível para todos os catálogos, exceto os criados via MCS.

Um fluxo de trabalho geral para usar arquivos CSV para adicionar máquinas em massa é o seguinte:

1. Na página **Máquinas**, selecione **Adicionar Arquivo CSV**. A janela **Adicionar Máquinas em Massa** é exibida.
2. Selecione **Baixar Modelo CSV**.
3. Preencha o arquivo de modelo.
4. Arraste ou navegue até o arquivo para carregá-lo.
5. Selecione **Validar** para realizar verificações de validação em sua importação.
6. Selecione **Importar** para concluir.

Para obter informações sobre considerações de arquivos CSV, consulte Considerações ao usar arquivos CSV para adicionar máquinas.

Você também pode exportar máquinas de um catálogo na mesma página Máquinas. O CSV exportado de máquinas pode então ser usado como um modelo ao adicionar máquinas em massa. Para exportar máquinas:

1. Na página **Máquinas**, selecione **Exportar para arquivo CSV**. Um arquivo CSV contendo uma lista das máquinas é baixado.

2. Abra o arquivo CSV para adicionar ou editar máquinas conforme necessário. Para adicionar máquinas em massa usando o arquivo CSV salvo, consulte a seção anterior, Usando arquivos CSV para adicionar máquinas em massa.

Nota:

- Este recurso não está disponível para catálogos de Acesso Remoto a PC.
- A exportação e importação de máquinas em arquivos CSV é suportada apenas entre catálogos do mesmo tipo.

Segurança

A página **Segurança** aparece apenas se você estiver criando um catálogo de máquinas sem atribuir um perfil de máquina em um ambiente de virtualização AWS. Use a página **Segurança** para configurar os grupos de segurança para as VMs. Isso também é aplicável ao editar e clonar um catálogo de máquinas existente.

Se você criar um catálogo de máquinas baseado em perfil de máquina, as configurações do grupo de segurança serão herdadas do perfil de máquina e a página **Segurança** não aparecerá.

Configurar NICs para as máquinas

A página **NICs** não aparece se você selecionar **Acesso Remoto a PC** na página **Tipo de Máquina**.

Se você planeja usar várias NICs, associe uma rede virtual a cada placa. Por exemplo, você pode atribuir uma placa para acessar uma rede segura específica e outra placa para acessar uma rede mais comumente usada. Você também pode adicionar ou remover NICs desta página.

Nota:

Para implantações VMware, ao criar um catálogo de máquinas usando um perfil de máquina, o catálogo herda as configurações de NIC do perfil de máquina. Nesses casos, se o perfil de máquina tiver várias NICs com a mesma rede, o Studio usará a rede da unidade de hospedagem para as configurações de NIC.

Adicionar contas de máquina

> **Nota:**
>
> Esta página **Contas de Máquina** aparece apenas quando você seleciona **Acesso Remoto a PC** na página **Tipo de Máquina**.

> Adicione as contas de máquina do Active Directory ou Unidades Organizacionais (OUs). Não use uma barra (/) em um nome de OU.

Você pode escolher uma conexão de gerenciamento de energia configurada anteriormente ou optar por não usar o gerenciamento de energia. Se você deseja usar o gerenciamento de energia, mas uma conexão adequada ainda não foi configurada, você pode criar essa conexão mais tarde e, em seguida, editar o catálogo de máquinas para atualizar as configurações de gerenciamento de energia.

Você também pode adicionar máquinas em massa usando arquivos CSV. Um fluxo de trabalho geral para fazer isso é o seguinte:

1. Na página **Contas de Máquina**, selecione **Adicionar Arquivo CSV**. A janela **Adicionar Máquinas em Massa** é exibida.
2. Selecione **Baixar Modelo CSV**.
3. Preencha o arquivo de modelo.
4. Arraste ou navegue até o arquivo para carregá-lo.
5. Selecione **Validar** para realizar verificações de validação em sua importação.
6. Selecione **Importar** para concluir.

Para obter informações sobre considerações de arquivos CSV, consulte Considerações ao usar arquivos CSV para adicionar máquinas.

Configurar identidades para máquinas no catálogo

> **Nota:**

- A página **Identidades da Máquina** aparece apenas quando você não seleciona **Acesso Remoto a PC** na página **Tipo de Máquina** e seleciona **Citrix Machine Creation Services (MCS)** na página **Gerenciamento de Máquina**.

Cada máquina no catálogo deve ter uma identidade exclusiva. Esta página permite configurar identidades para máquinas no catálogo. As máquinas são unidas à identidade após serem provisionadas. Você não pode alterar o tipo de identidade após criar o catálogo.

Um fluxo de trabalho geral para configurar as definições nesta página é o seguinte:

1. Selecione uma identidade na lista.
2. Indique se deseja criar contas ou usar as existentes, e o local (domínio) para essas contas.

Você pode selecionar uma das seguintes opções:

- **Active Directory local**: Máquinas pertencentes a uma organização e conectadas com uma conta do Active Directory que pertence a essa organização. Elas existem no local.

  Nota:

  Por padrão, o domínio onde o recurso (conexão) reside é selecionado.

- **Associado ao Microsoft Entra**: Máquinas pertencentes a uma organização e conectadas com uma conta do Microsoft Entra que pertence a essa organização. Elas existem apenas na nuvem. Para obter informações sobre os requisitos, limitações e considerações, consulte Associado ao Microsoft Entra.

  Nota:

  - Esta opção exige que a imagem mestre atenda ao pré-requisito do sistema operacional. Para obter mais informações, consulte a documentação da Microsoft Dispositivos associados ao Microsoft Entra.

- **Associado ao Microsoft Entra híbrido**. Máquinas pertencentes a uma organização e conectadas com uma conta do Active Directory Domain Services que pertence a essa

organização. Elas existem na nuvem e no local. Para obter informações sobre os requisitos, limitações e considerações, consulte Associado ao Microsoft Entra híbrido.

Nota:

- Antes de usar a associação híbrida do Microsoft Entra, certifique-se de que seu ambiente Azure atenda aos pré-requisitos. Consulte Configurar a associação híbrida do Microsoft Entra.
- Esta opção exige que a imagem mestre atenda ao pré-requisito do sistema operacional. Para obter mais informações, consulte Dispositivos associados ao Microsoft Entra híbrido.

- **Não associado ao domínio**. Máquinas não associadas a nenhum domínio. Para obter informações sobre os requisitos e limitações, consulte Não associado ao domínio.

Importante:

- Se você selecionar **On-premises Active Directory** ou **Microsoft Entra hybrid joined** como o tipo de identidade, cada máquina no catálogo deve ter uma conta de computador do Active Directory correspondente.
- O tipo de identidade **Non-domain-joined** requer a versão 1811 ou posterior do VDA como o nível funcional mínimo para o catálogo. Para torná-lo disponível, atualize o nível funcional mínimo.
- Os tipos de identidade **Microsoft Entra joined** e **Microsoft Entra hybrid joined** exigem a versão 2203 ou posterior do VDA como o nível funcional mínimo para o catálogo. Para torná-los disponíveis, atualize o nível funcional mínimo.
- Uma conta de serviço do Microsoft Entra é obrigatória ao criar catálogos somente Microsoft Entra ou Microsoft Entra registrados no Microsoft Intune para VMs persistentes e não persistentes.

Antes de configurar as identidades da máquina, certifique-se de ter permissão para criar contas de computador na UO onde as máquinas residem. Cada máquina no catálogo deve ter um nome exclusivo. Em seguida, escolha como configurar as identidades da máquina:

- Se você criar novas contas de máquina, especifique a UO e o esquema de nomenclatura da máquina. Para obter mais informações, consulte Esquema de nomenclatura de conta de máquina. Ao criar um catálogo, um pool de identidades é criado automaticamente para armazenar todas as identidades de máquina que você definiu para este catálogo.
- Se você usar contas de máquina existentes, escolha um pool de identidades existente em seu ambiente.

Nota:

Certifique-se de que os nomes das UOs não usem barras (`/`).

Ao criar um catálogo e selecionar **Usar pool de identidades existente** na página **Identidades da Máquina**, o comportamento da conta de serviço depende da configuração do pool de identidades:

- Se o pool de identidades selecionado não tiver uma conta de serviço configurada, a seleção de uma conta de serviço armazenada na página **Credenciais de domínio** não terá efeito. A operação **Adicionar máquinas** pode falhar com um erro indicando que a conta de serviço não pode ser encontrada. Para evitar isso, insira manualmente as credenciais de domínio na página **Credenciais de domínio**.
- Se o pool de identidades selecionado tiver uma conta de serviço configurada, qualquer conta de serviço selecionada na página **Credenciais de domínio** será ignorada. A operação **Adicionar máquinas** sempre usa a conta de serviço associada ao pool de identidades.

Se você usar contas existentes, navegue até as contas ou clique em **Importar** e especifique um arquivo `.csv` contendo nomes de contas. O conteúdo do arquivo importado deve usar o formato: `[ADComputerAccount] ADcomputeraccountname.domain`

Certifique-se de que haja contas suficientes para todas as máquinas que você está adicionando. O Studio gerencia essas contas. Portanto, permita que essa interface redefina as senhas de todas as contas ou especifique a senha da conta, que deve ser a mesma para todas as contas.

Para catálogos contendo máquinas físicas ou existentes, selecione ou importe contas existentes e atribua cada máquina a uma conta de computador do Active Directory e a uma conta de usuário.

Esquema de nomenclatura de contas de máquina

Cada máquina em um catálogo deve ter um nome exclusivo. Você deve especificar um esquema de nomenclatura de contas de máquina ao criar um catálogo. Use curingas (sinais de cerquilha) como espaços reservados para números ou letras sequenciais que aparecem no nome.

Ao especificar um esquema de nomenclatura, considere o seguinte:

- O número máximo de caracteres permitido é 15.
- O esquema de nomenclatura deve conter pelo menos um caractere curinga. Você deve colocar todos os curingas juntos.
- O nome completo, incluindo curingas, deve conter no mínimo 2 e no máximo 15 caracteres. Deve incluir pelo menos um caractere não numérico e um caractere # (curinga).
- O nome não deve incluir espaços ou qualquer um dos seguintes caracteres: `,~!@'$%\^&.()}{\/*?"<>|=+[];:_".`.
- O nome não pode terminar com um hífen (-).
- O número de caracteres aumenta com o aumento do número de contas de máquina. Por exemplo, se você criar 1.000 contas de máquina com o esquema "veryverylong#", o último nome de conta criado (veryverylong1000) conterá 16 caracteres, excedendo o número máximo de caracteres permitidos.

Você pode indicar se os valores sequenciais são números (0-9) ou letras (A-Z):

- **0-9**. Se selecionado, os curingas especificados se resolvem em números sequenciais.

  > **Nota:**
  >
  > Se houver apenas um curinga (#), os nomes das contas começam com 1. Se houver dois, os nomes das contas começam com 01. Se houver três, os nomes das contas começam com 001, e assim por diante.

- **A-Z**. Se selecionado, os curingas especificados se resolvem em letras sequenciais.

Por exemplo, um esquema de nomenclatura de PC-Sales-## (com **0-9** selecionado) resulta em contas nomeadas PC-Sales-01, PC-Sales-02, PC-Sales-03 e assim por diante.

Opcionalmente, você pode especificar com o que os nomes das contas começam.

- Se você selecionar **0-9**, as contas são nomeadas sequencialmente, começando com os números especificados. Insira um ou mais dígitos, dependendo de quantos curingas você usa no campo anterior. Por exemplo, se você usar dois curingas, insira dois dígitos ou mais.
- Se você selecionar **A-Z**, as contas são nomeadas sequencialmente, começando com as letras especificadas. Insira uma ou mais letras, dependendo de quantos curingas você usa no campo anterior. Por exemplo, se você usar dois curingas, insira duas letras ou mais.

Adicionar credenciais de domínio

Insira as credenciais de um administrador que tenha permissão para realizar operações de conta. As etapas detalhadas são as seguintes:

1. Clique em Inserir credenciais. A página Segurança do Windows é exibida.
2. No campo Nome de usuário, insira o SamName, nome de usuário ou SID do usuário do administrador. Dependendo da sua entrada:
    - Se você inserir um SamName, o campo **Domínio** será preenchido automaticamente.
    - Se você inserir um nome de usuário ou SID, poderá limitar a pesquisa de usuário a um domínio específico inserindo o nome do domínio ou SID no campo **Domínio**.
3. Clique em **Verificar nome** para verificar se o nome de usuário é válido ou exclusivo.
4. No campo **Senha**, insira a senha de domínio do administrador.
5. Clique em **Concluído**.

> **Nota:**
>
> Se o tipo de identidade selecionado em **Identidades da Máquina** for **Microsoft Entra híbrido unido**, as credenciais inseridas devem ter recebido a permissão `Write userCertificate`.

Selecione um conjunto de configuração WEM para Otimização da Experiência

> **Nota:**
>
> A página **Otimização da Experiência** aparece somente quando você tem um direito de Workspace Environment Management™ (WEM).

> Melhore a alocação de recursos e aprimore o desempenho do sistema em suas máquinas especificando um conjunto de configuração WEM para o catálogo de máquinas.

Permissões necessárias

Por padrão, a criação e o gerenciamento de conjuntos de configuração para catálogos de máquinas exigem a função de **Administrador Completo do WEM**, juntamente com uma das seguintes funções:

- **Administrador de Acesso Total**
- **Administrador de Nuvem**
- **Administrador de Catálogo de Máquinas**

Para permitir que outras funções gerenciem conjuntos de configuração, atribua a elas a permissão **Gerenciar conjuntos de configuração** e a função de **Administrador Completo do WEM**.

Pré-requisitos

Antes de vincular um catálogo a um conjunto de configuração, certifique-se de que sua implantação do serviço **Workspace Environment Management (WEM)** esteja configurada. Faça login no Citrix Cloud e inicie o serviço WEM. Para obter mais informações, consulte Introdução ao serviço Workspace Environment Management.

Se você já usa o WEM, verifique se o **agente WEM** está instalado em cada VDA e conectado ao Citrix Cloud para que as configurações de otimização possam ter efeito.

Etapas

Selecione uma opção de **Otimização da Experiência** para aplicar ao catálogo de máquinas:

- **Aplicar configurações padrão:** Selecione esta opção para aplicar as configurações de otimização padrão, incluindo proteção automática contra picos de CPU e otimização inteligente de CPU.
- **Aplicar configurações personalizadas:** Selecione esta opção para criar um conjunto de configurações para este catálogo de máquinas usando o nome do catálogo. Depois que o conjunto de configurações for criado, você poderá personalizar as configurações de otimização conforme necessário. Alternativamente, você pode selecionar um conjunto de configurações existente.

Atualizar VDA (opcional)

> **Importante:**

- Para garantir uma atualização tranquila, certifique-se de atender aos pré-requisitos e revisar os problemas conhecidos antes de atualizar os VDAs para as versões CR ou LTSR CU. Consulte Atualizar VDAs usando o Studio.
- Ao atualizar VDAs LTSR para versões de Atualização Cumulativa (CU) LTSR, certifique-se de que a versão dos Agentes de Atualização de VDA em execução nos VDAs seja 7.36.0.7 ou posterior. Para obter mais informações, consulte Atualizar VDAs usando o Studio.

Este recurso se aplica aos seguintes tipos de máquina:

- Máquinas persistentes provisionadas por MCS. Você as implanta usando **Citrix Machine Creation Services** na página **Gerenciamento de Máquinas** durante a criação do catálogo.
- Máquinas que não são criadas usando MCS (por exemplo, máquinas físicas). Você as implanta usando **Outro serviço ou tecnologia** na página **Gerenciamento de Máquinas** durante a criação do catálogo.

Para obter mais informações sobre as duas opções, consulte Gerenciamento de máquinas

Na página **Atualização de VDA**, selecione a versão do VDA para a qual deseja atualizar. Se especificado, os VDAs no catálogo que têm o Agente de Atualização de VDA instalado podem ser atualizados para a versão selecionada — imediatamente ou em um horário agendado.

Nota:

- Este recurso suporta a atualização apenas para o VDA mais recente. O momento em que você cria um agendamento de atualização de VDA ou atualiza um VDA determina a versão mais recente do VDA.
- Depois de configurar as configurações de atualização do VDA, pode levar até 15 minutos para que o campo **Atualização do VDA** reflita o status mais recente. Para exibir a coluna **Atualização do VDA**, clique no ícone Colunas a serem exibidas no canto superior direito, selecione **Catálogo de Máquinas > Atualização do VDA** e clique em **Salvar**.

Escolha uma trilha de VDA que se adapte à sua implantação:

> **Importante:**
>
> Você pode alternar entre o CR VDA e o LTSR VDA, desde que alterne de uma versão anterior para uma versão posterior. Você não pode alternar de uma versão posterior para uma versão anterior, pois isso é considerado um downgrade. Por exemplo, você não pode fazer downgrade de 2212 CR para 2203 LTSR (qualquer CU), mas pode fazer upgrade de 2112 CR para 2203 LTSR (qualquer CU).

- **CR VDA mais recente**. As Current Releases (CRs) oferecem os recursos e funcionalidades de virtualização de aplicativos, desktops e servidores mais recentes e inovadores.
- **LTSR VDA mais recente**. As Long Term Service Releases (LTSRs) são recomendadas para grandes ambientes de produção corporativos que preferem manter a mesma versão base por um período prolongado.

Após a criação do catálogo, você pode atualizar os VDAs conforme necessário. Para obter mais informações, consulte Atualizar VDAs.

Se você quiser habilitar a atualização do VDA mais tarde, poderá retornar a esta página editando o catálogo após a criação do catálogo. Para obter mais informações, consulte Configurar as configurações de atualização do VDA editando um catálogo.

Revisar as configurações

Na página **Resumo**, revise as configurações especificadas. Insira um nome e uma descrição para o catálogo. Essas informações aparecem no Studio.

Quando terminar, selecione **Concluir** para iniciar a criação do catálogo.

Em **Catálogos de Máquinas**, o novo catálogo aparece com uma barra de progresso em linha.

Para visualizar os detalhes do progresso da criação:

1. Passe o mouse sobre o catálogo de máquinas.
2. Na dica de ferramenta que aparece, clique em **Exibir detalhes**.

   Um gráfico de progresso passo a passo aparece onde você pode ver o seguinte:

   - Histórico de etapas
   - Progresso e tempo de execução da etapa atual

- Etapas restantes

Criar um catálogo de máquinas MCS usando comandos PowerShell

Você também pode criar um catálogo de máquinas MCS usando comandos PowerShell. Para obter mais informações, consulte:

- SDKs e APIs
- Gerenciar Citrix DaaS usando SDKs remotos do PowerShell
- New-ProvScheme

Atribuir uma letra de unidade específica a um disco de cache de write-back de E/S do MCS

Você pode atribuir uma letra de unidade específica a um disco de cache de write-back de E/S do MCS. Essa implementação ajuda a evitar conflitos entre a letra de unidade de quaisquer aplicativos que você usa e a letra de unidade do disco de cache de write-back de E/S do MCS. Para fazer isso, você pode usar comandos PowerShell. Os hipervisores suportados são Azure, GCP, VMware, SCVMM e XenServer.

> **Nota:**
>
> Este recurso requer a versão 2305 do VDA ou posterior.

Limitações

- Aplicável apenas ao sistema operacional Windows
- Letra de unidade aplicável para disco de cache de write-back: `E` a `Z`
- Não aplicável quando o disco temporário do Azure é usado como disco de cache de write-back
- Aplicável somente ao criar um novo catálogo de máquinas

Atribuir uma letra de unidade a um disco de cache de write-back

Para atribuir uma letra de unidade a um disco de cache de write-back:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Crie um pool de identidades, se ainda não tiver sido criado.

4. Crie um esquema de provisionamento usando o comando `New-ProvScheme` com a propriedade `WriteBackCacheDriveLetter`. Por exemplo:

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
```

```
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. Conclua a criação do catálogo.

Consideração importante sobre a configuração de propriedades personalizadas

As propriedades personalizadas devem ser definidas corretamente em `New-ProvScheme` e `Set-ProvScheme` em ambientes GCP e Azure. Se você especificar uma propriedade ou propriedades personalizadas inexistentes, receberá a seguinte mensagem de erro e os comandos falharão ao serem executados.

`Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.

Consideração importante sobre a configuração de parâmetros ProvScheme

Ao usar o MCS para criar um catálogo, você receberá um erro se:

- Definir os seguintes parâmetros `New-ProvScheme` em hipervisores não suportados ao criar um catálogo de máquinas:

PARÂMETRO	HIPERVISOR COMPATÍVEL
`UseWriteBackCache`	VMware

PARÂMETRO	HIPERVISOR COMPATÍVEL
	Hyper-V
	XenServer®
	Azure
	GCP
`DedicatedTenancy`	Azure
	GCP
	AWS
`TenancyType`	Azure
	GCP
	AWS
`UseFullDiskCloneProvisioning`	VMware
	Hyper-V
	XenServer

- Atualize os seguintes parâmetros `Set-ProvScheme` depois de criar o catálogo de máquinas:
  - `CleanOnBoot`
  - `UseWriteBackCache`
  - `DedicatedTenancy`
  - `TenancyType`
  - `UseFullDiskCloneProvisioning`

Adicionar SIDs ao criar máquinas virtuais

Você pode adicionar o parâmetro `ADAccountSid` para identificar exclusivamente as máquinas ao criar novas máquinas virtuais.

Para fazer isso:

1. Crie um catálogo com o tipo de identidade compatível.
2. Adicione máquinas ao catálogo usando `NewProvVM`. Por exemplo:

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

No entanto, você não pode provisionar uma máquina com:

- Uma conta AD que não está no pool de identidades do catálogo
- Uma conta AD que não está em estado disponível

Validar a configuração antes de criar um catálogo de máquinas MCS

Você pode validar as configurações antes de criar um catálogo de máquinas MCS usando o parâmetro `-validate` no comando `New-ProvScheme`. Depois de executar este comando PowerShell com o parâmetro, você receberá uma mensagem de erro apropriada se um parâmetro incorreto for usado ou se um parâmetro entrar em conflito com outro. Você pode então usar a mensagem de erro para resolver o problema e criar com sucesso um catálogo de máquinas MCS usando o PowerShell. Atualmente, este recurso é aplicável a ambientes de virtualização AWS, Azure, GCP e VMware.

Nota:

Durante a validação, você não deve criar um catálogo de máquinas MCS real. Você deve usar o resultado do comando para corrigir os erros e, em seguida, criar um catálogo bem-sucedido. Portanto, ao executar o comando `New-ProvScheme`, use um nome de pool de identidades falso.

Para validar a configuração, siga os passos abaixo:

1. Abra uma janela do PowerShell a partir do host do Delivery Controller.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute o comando `New-ProvScheme` e use o parâmetro `-validate`. Forneça um nome de pool de identidades falso para que o comando funcione. Por exemplo,

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg"
-IdentityPoolName``"mptmpcatalogdemo" -InitialBatchSizeHint 1  -
MasterImageVM "XDHyp:
\HostingUnits\vSanRg\Windows19MasterImage.``vm\Citrix_XD_NonMachineProf
ileWin19Machines.snapshot" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vSanRg\\VM Network.network"} -ProvisioningSchemeName`
`"MachineProfileW10Machines"  -Scope @()

-VMCpuCount 2  -VM

MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-Win11-
tpm-BL-TEMPLATE.``template" -TenancyType Shared  -FunctionalLevel
"L7_20" -Validate

$result.TerminatingError | Format-List -Property *
```

Mensagem de erro:

```
ErrorData    : {[[ValidationFailureCount, xxx], [InvalidMemoryValue,
The memory size provided 6143 must be a multiple of 4 MB and must be
greater than or equal to 4 MB.], [InconsistentGuestOsSetting, The
GuestOs setting - windows9_64Guest of the selected machine profile does
not match with the setting - windows2019srv_64Guest of master image.
Please select a machine profile that matches the GuestOs setting of the
master image.], [InconsistentVtpmSetting, The vTPM setting of the
selected machine profile does not match with the selected master image.
Please select a machine profile that matches the vTPM setting of the
master image.], [InconsistentFirmwareSetting, The firmware setting -
efi of the selected machine profile does not match with the setting -
bios of master image. Please select a machine profile that matches the
firmware setting of the master image ErrorId      : ValidationFailure

ErrorMessage : ValidationFailure

Operation    : ValidatingInputs
```

4. Após validar a configuração, você pode criar um catálogo de máquinas MCS com um nome de pool de identidades real e parâmetros corretos.

Integrar VMs ao Azure Arc

O Azure Arc permite que as organizações gerenciem recursos como VMs hospedadas em qualquer lugar como se estivessem sendo executadas no Azure. Com o Azure Arc, você pode usar serviços do Azure, como o Azure Monitor, para visibilidade abrangente e gerenciamento proativo dos recursos.

Para integrar VMs ao Azure Arc, crie um catálogo de máquinas MCS usando o comando `New-ProvScheme`. Você também pode atualizar um catálogo existente usando o comando `Set-ProvScheme`. Somente as novas VMs adicionadas ao catálogo são integradas ao Azure Arc.

Atualmente, este recurso é aplicável a todos os hipervisores Citrix locais VMware, Nutanix e SCVMM.

Pré-requisitos

Considere o seguinte antes de habilitar a integração do Azure Arc no catálogo MCS:

- Grupo de Recursos do Azure com:
  - Contas `Allows` para ler, criar e excluir servidores Arc.
  - Contas `Allows` para gerenciar extensões de VM, licenças e escopos de link privado.
  - Função `Azure Connected Machine Resource Administrator` atribuída ao principal de serviço no escopo do grupo de recursos.

Consulte Atribuir funções do Azure usando o portal do Azure.

- Imagem mestre com
  - VDA: Posterior a 2311, excluindo 2411.

    > **Nota:**
    >
    > A integração do Azure Arc não é suportada no Citrix Virtual Apps and Desktops 2411.

  - Agente AzureConnectedMachineAgent instalado. Você pode baixar o MSI nas seções Windows ou Linux da documentação da Microsoft.

Etapas para integrar VM ao Azure Arc

1. Configure uma conta de serviço com capacidade `AzureArcResourceManagement`.

A conta de serviço é usada para autenticação ou autorização, armazenando credenciais para acessar provedores de identidade como o Microsoft Entra ID. Cada conta de serviço está vinculada a um único provedor de identidade.

Para criar uma nova conta de serviço para acessar o Azure AD com `AzureArcResourceManagement capability`, execute:

```
New-AcctServiceAccount -IdentityProviderType “AzureAD”
-IdentityProviderIdentifier “tenant-id” -AccountId “application-id”
-AccountSecret “application-secret” -Capabilities
“AzureArcResourceManagement”
```

O `application-id` deve ser da mesma entidade de serviço à qual foi atribuída a função de Administrador de Recursos de Máquina Conectada do Azure.

2. Atribua a conta de serviço ao pool de identidades. Por exemplo:

```
Set-AcctIdentityPool -IdentityPoolUid “idn-pool-uid” -ServiceAccountUid
“service-account-uid”
```

3. Crie ou atualize um catálogo MCS com os seguintes parâmetros do Arc:

   - `EnableAzureArcOnboarding`: Indica se o Onboarding do Arc precisa ser habilitado no catálogo.
   - `AzureArcSubscriptionId`: Indica a assinatura do Azure onde as VMs conectadas ao Arc são criadas.
   - `AzureArcRegion`: Indica a região do Azure onde as VMs conectadas ao Arc são criadas.
   - `AzureArcResourceGroup`: Indica o grupo de recursos do Azure onde as VMs conectadas ao Arc são criadas. Consulte Pré-requisitos para obter informações sobre o Grupo de Recursos do Azure Arc.

   Exemplo: Para habilitar o Onboarding do Azure Arc para um novo catálogo:

```
`New-ProvScheme -ProvisioningSchemeName "demo" -MasterImageVM "XDHyp:
\HostingUnits\hosting-unit\masterVMName.vm\masterSnapshotName.snapshot"
-HostingUnitName “hosting-unit” -IdentityPoolName “identity-pool”`



-EnableAzureArcOnboarding -AzureArcSubscriptionId “azure-sub”
```

```
-AzureArcResourceGroup “azure-resourcegroup” - AzureArcRegion “azure-region”
```

Exemplo: Para habilitar o Onboarding do Azure Arc para um catálogo existente:

```
Set-ProvScheme -ProvisioningSchemeName "demo" -EnableAzureArcOnboarding $true -AzureArcSubscriptionId “azure-sub” -AzureArcResourceGroup “azure-resourcegroup” - AzureArcRegion “azure-region”
```

Exemplo: Para desabilitar o Onboarding do Azure Arc para um catálogo existente:

```
Set-ProvScheme -ProvisioningSchemeName "demo" -EnableAzureArcOnboarding $false:
```

4. Adicione novas máquinas ao catálogo para integrar o Arc.
5. Depois de ligar a VM, você deve ver a VM no portal do Azure em **AzureArcResourceGroup** como uma máquina conectada.

Considerações

- A integração do Arc é atualmente suportada apenas para novas VMs. Portanto, se você atualizar um catálogo existente usando `Set-ProvScheme`, apenas as VMs recém-adicionadas são integradas ao Arc quando ligadas pela primeira vez.
- As Propriedades Personalizadas do Arc ainda são suportadas para catálogos existentes para compatibilidade com versões anteriores. No entanto, se você executar `New-ProvScheme` com Propriedades Personalizadas do Arc, como `EnableAzureArcOnboarding`, a criação do catálogo falhará.
- Você deve adicionar todos os parâmetros em `New-ProvScheme` e `Set-ProvScheme` se configurar `EnableAzureArcOnboarding` como `true`.

Solução de problemas

Ao criar um catálogo SCVMM usando `New-ProvScheme`, você pode receber o seguinte erro:

```
Master Image/Machine Profile's VM's device id is different than the NetworkMapping's device id '0'. Please provide a device id that matches the master image/machine profile.
```

Nesse caso, certifique-se de especificar explicitamente o `DeviceId` no parâmetro `NetworkMapping` de `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeType "MCS" -InitialBatchSizeHint 1
-HostingUnitName $HostingUnitName `

            -IdentityPoolName $CatalogName -MasterImageVM $MasterImage
-ProvisioningSchemeName $CatalogName `

            -VMCpuCount 2 -VMMemoryMB 4096  -EnableAzureArcOnboarding `

            -AzureArcSubscriptionId $AzureArcSubscription -AzureArcRegion
$AzureArcRegion `

            -AzureArcResourceGroup $AzureArcResourceGroup

            -NetworkMapping @{"FDDxxxxxx-xxxx-4xxx-9EBC-3xxxxxxxx"="XDHyp:
\HostingUnits\<hosting unit name>\abc.network"}
```

Marcação Follow-Me

A marcação Follow-Me (Follow-Me Tagging) permite o rastreamento do uso individual de VMs por usuários finais, aplicando tags em nível de hipervisor. Essas tags, rotuladas com o usuário e/ou organização específicos (usando `citrix-user-upn` como chave e o Nome Principal do Usuário (UPN) como valor), são adicionadas automaticamente pelo Citrix quando um usuário é atribuído a uma VM e removidas quando o usuário é desatribuído.

Vantagens

Este recurso oferece várias vantagens:

- **Rateio de custos de TI**: Facilita a filtragem do uso de recursos (Azure: NICs, SO, ID, WBC, discos de dados e VMs) (AWS EC2: instância EC2, volumes EBS (SO, ID, WBC e discos de dados) e NICs) por tags, permitindo um rateio de custos preciso para usuários individuais ou unidades de negócios.

> **Nota:**

  - Para AWS EC2, ative a chave de tag `citrix-user-upn` como uma tag de alocação de custos para que ela apareça no seu relatório de faturamento. Consulte Ativando tags geradas pela AWS como tags de alocação de custos.
  - Para Azure, você não precisa ativar a tag `citrix-user-upn` para filtrar relatórios de análise de custos por usuário e visualizar gastos detalhados, que incluem, gasto total mensal, custos por recurso individual, tendências de custos diárias, custos por serviço e registros de faturamento detalhados.

- **Gerenciamento eficiente de usuários**: Automatiza a remoção de tags de recursos quando os usuários finais são desatribuídos (por exemplo, mudanças de emprego como rescisão ou reorganização).
- **Monitoramento de segurança aprimorado**: Ajuda a identificar VMs atribuídas a usuários finais específicos para verificações de segurança direcionadas.

Aplicabilidade

Atualmente, a marcação follow-me é aplicável a:

- Ambientes AWS EC2 e Azure
- Máquinas atribuídas estaticamente executando SO de sessão única
- Catálogos persistentes e não persistentes
- Todos os catálogos com identidade de máquina suportados
- Apenas VMs provisionadas por MCS
- Apenas discos gerenciados (para Azure)

Limitações

- Existe um breve período de sincronização entre a atribuição do usuário final e o aparecimento da tag correspondente na máquina do hipervisor.
- O MCS não tenta novamente as operações de marcação se a operação de marcação falhar devido a problemas como permissões de marcação insuficientes, falhas do hipervisor ou Cloud Connectors indisponíveis. Em vez disso, o MCS emite um aviso no esquema de provisionamento. Este aviso pode ser acessado usando o comando PowerShell `Get-ProvOperationEvent`.
- As operações de tag são iniciadas exclusivamente quando a marcação de um catálogo é ativada ou desativada, ou quando um usuário é atribuído a uma VM.

- Se você remover manualmente a tag follow-me da NIC, a tag não será aplicada a nenhum recurso recém-criado no próximo ligar.

Considerações importantes

Considere o seguinte ao usar a marcação follow-me em ambientes AWS EC2:

- Limitações específicas da AWS: Consulte Limitações de marcação para limitações de marcação.
- Ative a marcação para alocação de custos. Consulte Ativando tags de alocação de custos geradas pela AWS.

Considere o seguinte ao usar a marcação follow-me no ambiente Azure:

- Limitações específicas do Azure
- Você pode adicionar apenas 50 tags por recurso.

Configurar a marcação follow-me

Você pode configurar a marcação follow-me usando (#use-studio) e (#use-powershell).

Usar o Studio

No assistente de Configuração do Catálogo de Máquinas:

1. Na página **Sistema Operacional**, selecione **SO de sessão única.**
2. Na página **Gerenciamento de Máquinas**:
    - Selecione **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade).**
    - Selecione para implantar máquinas usando a **tecnologia de provisionamento Citrix Machine Creation Services (MCS)**.
3. Conclua as configurações nas páginas a seguir.
4. Na página **Máquinas Virtuais**, selecione **Aplicar marcação follow-me**.
5. Conclua o processo de criação do catálogo.
6. Para verificar se o recurso está habilitado para o catálogo, navegar até a página **Detalhes** do catálogo criado. A capacidade **Marcação follow-me** em **Máquina** deve aparecer como **Habilitado**.

7. No painel esquerdo, selecione **Grupos de entrega**, clique em **Criar Grupo de Entrega**. Adicione o catálogo criado a um grupo de entrega e atribua um ou mais usuários ao grupo de entrega.

O MCS marca automaticamente uma VM no catálogo com o primeiro usuário que faz logon na máquina. Alternativamente, os usuários podem ser atribuídos manualmente a uma máquina em vez de depender do primeiro logon.

Você também pode editar um catálogo existente para configurar a marcação follow-me.

1. Selecione o catálogo que deseja modificar e clique em **Editar Catálogo de Máquinas**.
2. navegar até a seção **Máquinas Virtuais** e selecione **Aplicar Marcação Follow-me**.
3. Clique em **Aplicar** e depois em **Salvar** para habilitar o recurso para o catálogo existente. VMs novas e existentes neste catálogo agora são marcadas no hipervisor quando os usuários finais são atribuídos.

Usar PowerShell

Para configurar a marcação follow-me usando PowerShell, use o parâmetro `-HypervisorVMTagging` com o cmdlet `Set-BrokerCatalog` e defina-o como `$true`.

Exemplo de script para habilitar a marcação:

```
Set-BrokerCatalog -Name 'CatalogName' -HypervisorVMTagging $true
```

Exemplo de script para verificar o status da marcação de um catálogo:

```
Get-BrokerCatalog -Name "SS-S-P-Cat" | Select Name, SessionSupport,
AllocationType, ProvisioningType, HypervisorVMTagging
```

Verifique o valor de `HypervisorVMTagging`. Se a marcação follow-me estiver habilitada para o catálogo, o valor de `HypervisorVMTagging` será `True`.

Depois de habilitar a marcação follow-me para o catálogo, adicione o catálogo criado a um grupo de entrega e atribua um ou mais usuários ao grupo de entrega.

Usar a marcação follow-me

Depois de habilitar a marcação follow-me para um catálogo de máquinas e os usuários serem atribuídos às VMs dentro desse catálogo, o MCS aplica automaticamente uma tag de nível de hipervisor às máquinas virtuais. Esta tag está no formato `citrix-user-upn:<User Principal`

`Name (UPN)>`. Use esta tag no console de faturamento e gerenciamento do seu hipervisor para rastrear o uso de recursos por usuários finais específicos.

Para analisar os custos de recursos com tags específicas no Azure:

1. Vá para a página **Análise de Custos** no Portal do Azure.
2. Adicione o filtro **Tag**.
3. Use `citrix-user-upn` como a chave.
4. Selecione um ou mais UPNs desejados para rastrear os custos de recursos.
5. Visualize os custos reais acumulados para os recursos marcados.

Use a filtragem de tags com `citrix-user-upn` para:

- Ver o gasto total mensal de um usuário (visualização de custos acumulados).
- Visualizar todos os recursos de propriedade de um usuário específico e seus custos (visualização de custo por recursos).
- Detectar aumentos inesperados nos custos diários por usuário (visualização de custos diários).
- Identificar em quais serviços um usuário está gastando, como VMs ou Armazenamento (visualização de custo por serviço).
- Construir registros detalhados de faturamento em nível de usuário filtrando itens de linha de faturamento brutos (visualização de detalhes da fatura).

Para analisar custos de recursos com tags de alocação de custos no AWS:

1. Ative as tags de alocação de custos (leva até 24 horas para serem ativadas e ficarem visíveis no Relatório de Faturamento). Ative as tags de alocação de custos através do console de faturamento do EC2 ou da API do AWS cost explorer, `UpdateCostAllocationTagsStatus`.
2. Adicione a Chave da Tag de alocação de custos e algum valor aos recursos do AWS.

Usando essas tags, gere os relatórios de faturamento para visualizar o custo incorrido pelos recursos de acordo com a chave da tag de alocação de custos e valores específicos. Você pode visualizar o relatório com granularidade mensal, diária e horária.

Quando um usuário é desatribuído de uma máquina, o MCS remove automaticamente a tag correspondente dessa VM.

Solução de problemas

- **Problema**: As tags não estão aparecendo no hipervisor após a atribuição do usuário.

- **Causa**: Pode haver um atraso na sincronização, ou o MCS falhou ao realizar a marcação devido a problemas de permissão, falha do hipervisor ou Cloud Connectors indisponíveis.
- **Solução**:
  - Aguarde alguns minutos para que a tag apareça.
  - Se o problema persistir, verifique se há avisos no esquema de provisionamento usando o cmdlet do PowerShell `Get-ProvOperationEvent` para identificar quaisquer erros encontrados durante a marcação. Certifique-se de que a Citrix tenha as permissões de marcação necessárias no hipervisor.
  - Verifique o status da marcação. Execute `Get-ProvVM` e verifique o `CustomMachineData` para o Booleano `IsFollowMeTagged`.

Replicação de imagem de armazenamento adicional para hipervisores locais suportados

Este recurso permite a replicação e o gerenciamento eficientes de instâncias de especificação de versão de imagem em vários locais de armazenamento suportados por hipervisores locais.

Casos de uso

- Você pode replicar versões de imagem para locais de armazenamento novos ou substituídos, permitindo que máquinas virtuais sejam provisionadas em locais adicionais durante ou após o processo de preparação da imagem.
- Quando uma nova versão de imagem é criada e locais de armazenamento adicionais são especificados, a especificação da versão de imagem preparada é automaticamente replicada para esses locais de armazenamento designados.
- Se houver a necessidade de usar uma versão de imagem existente com locais de armazenamento substituídos ou recém-adicionados, você pode adicionar uma instância de versão de imagem para replicar para o novo local de armazenamento.
- Quando uma unidade de hospedagem é adicionada a uma versão de imagem existente, juntamente com armazenamento adicional, a instância da especificação da versão de imagem preparada será replicada para os armazenamentos adicionais especificados dentro da unidade de hospedagem de destino.

Comandos PowerShell

- Adicione uma nova instância de imagem que replica uma especificação de versão de imagem preparada para o local de armazenamento especificado.

```
Add-ProvImageVersionSpecInstance -ImageVersionSpecUid <
ImageVersionSpecUid > -StorageIds "<StorageId1,StorageId2>"
-RunAsynchronously
```

- Remova uma réplica de instância de especificação de versão de imagem existente e não usada por nenhuma VM existente.

```
Remove-ProvImageVersionSpecInstance -ImageVersionSpecUid <
ImageVersionSpecUid >  -ImageInstanceUid < ImageInstanceUid >
-RunAsynchronously
```

- Obtenha uma lista de instâncias de especificações de versão de imagem.

```
Get-ProvImageVersionSpecInstance -ImageVersionSpecUid  <
ImageVersionSpecUid >
```

Onde ir em seguida

Para obter informações sobre a criação de catálogos de hipervisor específicos, consulte:

- Criar um catálogo AWS
- Criar um catálogo Google Cloud Platform
- Criar um catálogo Microsoft Azure
- Criar um catálogo Microsoft System Center Virtual Machine Manager
- Criar um catálogo Nutanix
- Criar um catálogo VMware
- Criar um catálogo XenServer

Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.

Para revisar todo o processo de configuração, consulte Planejar e construir uma implantação.

Você pode criar um catálogo do Citrix Provisioning usando o Studio e o PowerShell. Esta implementação oferece as seguintes vantagens:

- Um único console unificado para gerenciar catálogos MCS e Citrix Provisioning.
- Ter novos recursos para catálogos do Citrix Provisioning, como solução de gerenciamento de identidade, provisionamento sob demanda e assim por diante.

Atualmente, este recurso está disponível apenas para cargas de trabalho do Azure e VMware. No entanto, em ambientes VMware e XenServer, você pode atualmente criar os catálogos usando apenas comandos do PowerShell. Para obter mais informações, consulte Criar catálogos do Citrix Provisioning no Citrix Studio.

Mais informações

- Gerenciamento de Imagens do Citrix Virtual Apps and Desktops
- Criar e gerenciar conexões e recursos
- Pools de identidade de diferentes tipos de junção de identidade de máquina
- Gerenciar catálogos de máquinas

Criar um catálogo de instâncias gerenciadas do Amazon WorkSpaces Core

(/pt-br/citrix-daas/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos das instâncias gerenciadas do Amazon WorkSpaces Core.

> **Nota:**
>
> Atualmente, a criação de catálogos de VMs persistentes e não persistentes (a propriedade `CleanOnBoot` é `True` ou `False`) é suportada.

Pré-requisitos

Antes de criar um catálogo de instâncias gerenciadas do Amazon WorkSpaces Core, você precisa concluir a criação de:

1. Uma conexão com as instâncias gerenciadas do Amazon WorkSpaces Core. Consulte Conexão com instâncias gerenciadas do Amazon WorkSpaces Core
2. Uma imagem preparada. Consulte Criar uma imagem preparada para instâncias gerenciadas do Amazon WorkSpaces Core.

Configuração de rede durante a preparação da imagem

Durante a preparação da imagem, uma máquina virtual (VM) de preparação é criada com base na VM original. Esta VM de preparação é desconectada da rede. Para desconectar a rede da VM de preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e

saída. Este grupo de segurança de rede persiste e é reutilizado. O nome do grupo de segurança de rede é `Citrix.XenDesktop.IsolationGroup-GUID`, onde GUID é gerado aleatoriamente.

Um catálogo de máquinas baseado em perfil de máquina

Você pode usar um perfil de máquina para capturar as propriedades de hardware de uma instância EC2 (VM) ou versão de modelo de inicialização e aplicá-las às máquinas provisionadas. As propriedades capturadas podem incluir, por exemplo, tipo de locação, tipo de instância, grupos de segurança, mapeamentos de rede, propriedades de volume EBS, otimização EBS, opções de CPU, capacidade de hibernação e outras configurações AWS suportadas.

Você pode usar uma instância AWS EC2 (VM) ou uma versão de modelo de inicialização AWS como entrada do perfil da máquina.

> **Nota:**
>
> - As propriedades do volume EBS são derivadas apenas de um perfil de máquina.
> - O Serviço de Metadados de Instância (IMDS) V2 é o único suportado, e não o IMDS V1. Para obter informações, consulte Como funciona o Serviço de Metadados de Instância Versão 2.

Tenancy da AWS

A AWS oferece as seguintes opções de tenancy: tenancy compartilhada (o tipo padrão) e tenancy dedicada. Tenancy compartilhada significa que várias instâncias do Amazon WorkSpaces Core de diferentes clientes podem residir na mesma peça de hardware físico. Tenancy dedicada significa que suas instâncias do Amazon WorkSpaces Core são executadas apenas em hardware com outras instâncias que você implantou.

> **Nota:**
>
> Somente as instâncias dedicadas são suportadas (hosts dedicados não são suportados atualmente). Outros clientes não usam a mesma peça de hardware.

O tipo de tenancy é capturado do perfil da máquina

Ao usar o MCS para criar um catálogo para provisionar máquinas na AWS, o tipo de tenancy é capturado do perfil da máquina.

- **Hardware compartilhado**: Essa configuração é adequada para a maioria das implantações. Vários clientes compartilham peças de hardware, mesmo que não interajam entre si. Usar hardware compartilhado é a opção menos dispendiosa para executar suas instâncias do Amazon EC2.
- **Instância dedicada**: Essa configuração é mais adequada para implantações com requisitos específicos de segurança ou conformidade. Com uma instância dedicada, você ainda desfruta dos benefícios de ter um host separado de outros clientes da AWS, mas não paga pelo host inteiro. Você não precisa se preocupar com a capacidade do host, mas é cobrado a uma taxa mais alta pelas instâncias. Além disso, as Instâncias Dedicadas fornecem suporte limitado para Traga Sua Própria Licença (BYOL).

Faturamento flexível

O Amazon WorkSpaces Core Managed Instances suporta dois modos de faturamento:

MODO DE FATURAMENTO	DESCRIÇÃO
Mensal	Faturamento fixo, mensal e com taxa fixa. Ideal para desktops persistentes e cargas de trabalho previsíveis.
Por hora	Faturamento pré-pago. Esta é a configuração padrão da AWS se nenhum modo de faturamento for explicitamente especificado.

Essas opções oferecem flexibilidade para gerenciar os custos de computação com base na persistência e nos padrões de uso da sua carga de trabalho.

Este recurso requer o uso do serviço de faturamento do Amazon WorkSpaces. Por padrão, o MCS usa este serviço para provisionar e gerenciar instâncias, permitindo que você se beneficie de preços de taxa fixa mais competitivos para cargas de trabalho persistentes.

Pré-requisitos e considerações

- Configuração da conta AWS: Sua conta AWS deve ser configurada para usar o serviço de faturamento do WorkSpaces. Embora as contas AWS sejam alteradas por padrão, alguns clientes podem solicitar que a AWS permaneça no serviço de faturamento EC2 legado para usar instâncias gerenciadas do WorkSpaces Core.

> **Nota:**

> Se sua conta estiver no serviço de faturamento EC2 legado, a opção de faturamento **Mensal** não estará disponível.

- Conexão do host: O faturamento flexível é aplicável apenas a conexões de host do Amazon WorkSpaces Core. Não é compatível com conexões de host padrão do AWS EC2.
- Instâncias spot: As instâncias spot não são compatíveis com o serviço de faturamento do WorkSpaces.
- Faturamento misto: Uma conta AWS deve usar o faturamento do WorkSpaces ou o faturamento do EC2 para instâncias gerenciadas principais. Uma combinação de ambos em uma única conta não é compatível.
- Compatibilidade: Apenas tipos de instância, tipos de plataforma (SO) e tipos de locação específicos são compatíveis com determinados modos de faturamento. O MCS executa uma verificação pré-voo para garantir que suas seleções (Oferta de Serviço, Perfil de Máquina e Imagem Preparada) correspondam ao modo de faturamento escolhido.

Consulte Criar um catálogo de máquinas com um modo de faturamento específico.

Criar um catálogo

Uma imagem preparada e um perfil de máquina são necessários para criar catálogos de instâncias gerenciadas do Amazon WorkSpaces Core. Você pode usar uma instância de VM da AWS ou uma versão de modelo de inicialização da AWS como entrada do perfil de máquina.

Você pode criar um catálogo usando:

- Studio
- PowerShell

Criar um catálogo usando o Studio

Criar um catálogo de máquinas a partir do nó Imagens

Use a opção **Criar catálogo** no nó **Imagens** para criar um catálogo usando a versão da imagem.

Alternativamente, você pode selecionar a versão ao criar um catálogo no nó **Catálogos de Máquinas**, vinculando à opção de imagem preparada no fluxo de trabalho de criação de catálogo. Consulte Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas.

Para criar um catálogo de máquinas MCS a partir do nó **Imagens**, faça o seguinte:

1. Selecione uma versão da imagem e clique em **Criar catálogo**. Clique em **Avançar** na página **Introdução**.
2. Nas páginas **Gerenciamento de Máquinas** e **Imagem**, as configurações são pré-selecionadas com base na versão da imagem selecionada. Na página Imagem, insira uma nota para a imagem preparada selecionada.
3. Conclua as configurações nas páginas seguintes.
4. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.
5. Vá para o nó **Catálogos de Máquinas** para ver o catálogo de máquinas criado.

Criar um catálogo de máquinas a partir do nó Catálogos de Máquinas

Para criar um catálogo de máquinas MCS a partir do nó Catálogos de Máquinas, faça o seguinte:

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo.
2. Clique em **Criar Catálogo de Máquinas**. A página **Configuração do Catálogo de Máquinas** é exibida.
3. Na página **Tipo de Máquina**, selecione um tipo de máquina para o catálogo, por exemplo, **SO de Multi-sessão**.
4. Na página **Gerenciamento de Máquinas**, selecione as seguintes configurações:
    a. Selecione **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade)**.
    b. Selecione **Tecnologia de provisionamento Citrix**. Em seguida, selecione **Citrix Machine Creation Services™**.
    c. No campo **Recursos**, selecione os recursos (Zona de Disponibilidade ou Zona Local) que você configurou ao criar a conexão do host e clique em **Avançar**.
5. Na página **Experiência da área de trabalho**, selecione uma área de trabalho aleatória ou estática que você deseja que os usuários tenham ao fazer login. Se uma área de trabalho estática for selecionada, especifique ainda se deseja salvar as alterações que o usuário faz no disco local (persistente ou não persistente).
6. Na página **Imagem**, clique em **Selecionar uma imagem** para selecionar uma imagem preparada para o catálogo de máquinas. Selecione a versão preparada que você criou. Clique no nome da versão da imagem. Para ver mais detalhes sobre a versão da imagem selecionada, clique no número da versão, que está sublinhado. Clique em **Concluído**.

O perfil da máquina associado à imagem preparada é exibido e suas propriedades de hardware (por exemplo, tipo de instância, tipo de locação, mapeamentos de rede, grupos de segurança, propriedades de volume) são usadas para criar máquinas nos catálogos. Para alterar a origem do perfil da máquina para outra VM ou versão do modelo de inicialização, clique no botão editar.

7. Na página **Máquinas Virtuais**:
    a. Insira o número de VMs para o catálogo.
    b. A especificação padrão da máquina é exibida, que se baseia no perfil da máquina. Para alterá-la, selecione o ícone de edição e selecione uma especificação de máquina.
8. Na página **NICs**, selecione as NICs (ou ENIs) para as VMs.
9. Na página **Identidades da Máquina**, configure o tipo de identidade da máquina para as máquinas no catálogo:
    a. Para configurar **máquinas ingressadas no domínio (Active Directory local ou Microsoft Entra híbrido)**, selecione o domínio e crie novas contas AD para as VMs a serem criadas neste catálogo de máquinas. As VMs provisionadas são ingressadas no domínio selecionado. Para provisionar **máquinas não ingressadas no domínio**, selecione a opção de não ingresso no domínio.
    b. Especifique o esquema de nomenclatura de contas para as novas contas a serem criadas para as VMs.
10. Na página **Credenciais de domínio**, clique em **Inserir credenciais** para fornecer as credenciais para o domínio selecionado. Insira o nome de usuário e a senha de nível de administrador quando solicitado. Você também pode usar uma conta de serviço se já salvou credenciais de domínio anteriormente, seguindo nossa documentação do produto.
11. Clique nas páginas restantes até a página **Resumo**. Insira um nome para o catálogo de máquinas e selecione **Concluir** para criar o catálogo de máquinas.

Limitações na criação de um catálogo de máquinas em uma zona local da AWS

- Certas zonas locais suportam apenas determinadas configurações de hardware (por exemplo, a zona local de Perth não suporta volumes GP3, apenas GP2).
- Como apenas gp2 é universalmente suportado em todas as zonas locais, e nem todas suportam gp3, a criação de disco de ID padroniza o uso do tipo de volume gp2.
- Você deve selecionar um perfil de máquina com especificações de hardware que são suportadas na zona local desejada.

- Snapshots de AMIs de imagem preparada e snapshots de disco de ID padronizam ser colocados na região, em vez da zona local (devido a limitações da AWS em relação à visibilidade do suporte a snapshots EBS em zonas locais).
- Apenas zonas locais que suportam serviços EC2 e EBS completos são zonas suportadas.

Criar um catálogo usando PowerShell

Criar um catálogo usando uma especificação de versão de imagem preparada e perfil de máquina

- Crie um catálogo de máquinas não persistentes MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$true] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

- Crie um catálogo de máquinas persistentes MCS a partir da especificação de versão de imagem preparada usando o comando `New-ProvScheme`. Por exemplo,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-CleanOnBoot
$false] [-MachineProfile <string>] [-ProvisioningSchemeType “MCS”]
```

Exemplo do conjunto completo de comandos Powershell para criar um catálogo:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "wsccatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "domainname"
-IdentityPoolName "wsccatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "aws##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
```

```
$Task = New-ProvScheme -ProvisioningSchemeName wsccatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName wsc -IdentityPoolName wsccatalog -CleanOnBoot -Scope @()
-SecurityGroup @() -MachineProfile 'XdHyp:\HostingUnits\cvad-test-
scalestress\us-east-1a.availabilityzone\machine-profile-instance i
(i-0xxxxxxxx).vm' -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName wsccatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

Atualizar o perfil da máquina

Para atualizar o perfil da máquina em um catálogo que foi inicialmente provisionado com um perfil de máquina, faça o seguinte. Você também pode alterar o tipo de locação e a capacidade de hibernação da origem do perfil da máquina ao editar um catálogo de máquinas MCS.

1. Execute o comando `Set-ProvScheme`. Por exemplo,

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

Criar um catálogo de máquinas com um modo de cobrança específico

Atualmente, você pode especificar o modo de cobrança ao criar um catálogo de máquinas usando apenas o PowerShell.

USAR POWERSHELL

Para especificar o modo de cobrança via PowerShell, use o parâmetro `CustomProperties` no comando `New-ProvScheme`.

```
$custprop = "BillingMode,Monthly"



New-ProvScheme -ProvisioningSchemeName "MyCatalog" `

-ImageVersionSpecUid $ImageVersionSpecUid `

-HostingUnitName "wsc-unit" `

-IdentityPoolName "MyIdentityPool" `

-MachineProfile "XdHyp:\HostingUnits\wsc-unit\machine-profile
lt-123.launchtemplate\lt-123 (1).launchtemplateversion" `

-CustomProperties $custprop `

-CleanOnBoot
```

> **Nota:**
>
> Se a propriedade `BillingMode` for omitida, o catálogo usará `Hourly` como padrão.

Alterar o modo de cobrança de um catálogo existente

Você pode converter um catálogo existente de `Monthly` para `Hourly`, ou vice-versa. Essa alteração pode ser aplicada a VMs novas e existentes no catálogo.

CONSIDERAÇÕES IMPORTANTES PARA ATUALIZAÇÕES

- Janela de serviço: As VMs existentes devem passar por uma janela de serviço ou ciclo de energia para aplicar a alteração de cobrança.
- Validação: O MCS valida se os tipos de instância e plataformas existentes são compatíveis com o novo modo de cobrança antes de aplicar a alteração.

ATUALIZAR USANDO POWERSHELL

- Para atualizar o modo de cobrança apenas de novas VMs adicionadas a um catálogo, atualize a propriedade personalizada do modo de cobrança do esquema de provisionamento:

```
$custprop = "BillingMode,Hourly"



Set-ProvScheme -ProvisioningSchemeName "MyCatalog" -CustomProperties
$custprop
```

- Para atualizar o modo de cobrança de VMs novas e existentes em um catálogo, crie uma nova versão do esquema de provisionamento com a propriedade personalizada atualizada e aplique a nova versão a todas as VMs:

```
$custprop = "BillingMode,Hourly"



New-ProvSchemeVersion -ProvisioningSchemeName "MyCatalog"
-CustomProperties $custprop



New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 2 `

-StartsNow -AllVMs `

-MaxDurationInMinutes 100 `

-ProvisioningSchemeName "MyCatalog"
```

Monitorar informações de cobrança

Você pode verificar o modo de cobrança para catálogos e máquinas virtuais individuais.

Execute os seguintes comandos PowerShell para verificar a elegibilidade de cobrança da sua conta:

- Retorna `BillingMode` como parte de CustomProperties

```
Get-ProvScheme –ProvisioningSchemeName “"MyCatalog" "  | Select
 ProvisioningSchemeName,  CustomProperties
```

- Retorna `BillingMode` como parte de VMInfo

```
Get-ProvVMDetails –ProvisioningSchemeName “"MyCatalog" "  | Select-
Object  -ExpandProperty VMInfo
```

Solução de problemas e validação

O MCS inclui verificações pré-voo para evitar configurações incompatíveis. Você pode encontrar os seguintes erros durante a criação ou edição do catálogo:

- **NoInstanceConfigFoundForBillingMode**: Ocorre se a Oferta de Serviço (tipo de instância), Tenancy e Tipo de Plataforma selecionados não forem suportados para o modo de cobrança escolhido.
- **Instância Spot Não Suportada**: Se você tentar usar instâncias Spot com uma conexão de host do WorkSpaces, a validação falhará.
- **Restrição de cobrança do EC2**: Se sua conta AWS estiver no modelo de cobrança EC2 legado, tentar definir um modo de cobrança Mensal resultará em um erro de validação.

Criar um catálogo com versão de modelo de inicialização usando PowerShell

Você pode criar um catálogo de máquinas MCS com uma versão de modelo de inicialização como entrada de perfil de máquina. Você também pode atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização e de uma versão de modelo de inicialização para uma VM.

No console do AWS EC2, você pode fornecer as informações de configuração da instância de um modelo de inicialização junto com o número da versão. Quando você especifica a versão do modelo de inicialização como entrada de perfil de máquina ao criar ou atualizar um catálogo de máquinas, as propriedades dessa versão do modelo de inicialização são copiadas para as VMs VDA provisionadas.

As seguintes propriedades podem ser fornecidas usando a entrada do perfil da máquina ou explicitamente como parâmetros nos comandos `New-ProvScheme` ou `Set-ProvScheme`. Se forem fornecidas nos comandos `New-ProvScheme` ou `Set-ProvScheme`, elas terão precedência sobre os valores do perfil da máquina dessas propriedades.

- Oferta de Serviço

- Redes

> **Nota:**

> Se a oferta de serviço não for fornecida no modelo de inicialização do perfil da máquina ou como um parâmetro no comando `New-ProvScheme`, você receberá um erro apropriado.

> Para criar um catálogo usando a versão do modelo de inicialização como entrada de perfil da máquina:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Obtenha a lista de versões de um modelo de inicialização. Por exemplo:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. Crie um pool de identidades, se ainda não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. Crie um esquema de provisionamento com uma versão de modelo de inicialização como entrada de perfil da máquina. Por exemplo:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `
```

```
-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-ImageVersionSpecUid ‘24dfb047-e867-527g-896c-25664xxxxx1t’ `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. Registre um esquema de provisionamento como um catálogo de broker. Por exemplo:

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. Conclua a criação do catálogo.

Atualizar a origem do perfil da máquina

Você também pode atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização e de uma versão de modelo de inicialização para uma VM. Por exemplo:

- Para atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
```

```
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- Para atualizar a entrada de um catálogo de perfil de máquina de uma versão de modelo de inicialização para uma VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

Catálogo habilitado para MCSIO

A Otimização de Armazenamento MCS (MCSIO) melhora o desempenho da VM armazenando em cache as operações de disco na memória ou em um disco pequeno de alta velocidade. Você pode criar um catálogo não persistente habilitado para MCSIO usando comandos PowerShell. Para criar tal catálogo, você deve instalar o driver MCSIO durante a instalação ou atualização do VDA durante a preparação da instância AMI. Por padrão, esse driver não é instalado.

Depois que uma AMI MCSIO é preparada (ao instalar o VDA, selecione a opção para incluir o driver MCSIO na instalação), você pode criar um catálogo não persistente habilitado para MCSIO.

> **Nota:**
>
> A opção de configurar o MCSIO com apenas cache de disco (sem cache de memória) usando o Studio foi removida em todos os hipervisores e ambientes de serviço de nuvem.

Criar um catálogo habilitado para MCSIO

Os quatro parâmetros adicionados ao comando PowerShell New-ProvScheme são:

- `UseWriteBackCache`: Ativa o cache (cache de write-back) para o esquema de provisionamento fornecido
- `WriteBackCacheDiskSize`: Especifica o tamanho em GB do disco temporário usado para cache
- `WriteBackCacheMemorySize`: Especifica a quantidade de memória em MB a ser usada para cache. Este é um parâmetro opcional.

Nota:

- O valor de `WriteBackCacheDiskSize` deve ser maior que zero porque é necessário pelo menos 1 GB de armazenamento em disco de cache. O tamanho do disco de cache não deve ser maior que o tamanho do disco do SO.
- O valor de `WriteBackCacheMemorySize` deve ser diferente de zero e menor que o tamanho da memória do catálogo de máquinas.

As propriedades personalizadas que afetam o MCSIO são:

- `WBCDiskStorageType`: Define o tipo de volume, que é usado para o disco temporário em instâncias gerenciadas do Amazon WorkSpaces Core. Este parâmetro aceita um argumento de string no formato `volume-type[:iops][:throughput]`. A seguir estão os tipos de volume:
  - gp2: Não use os parâmetros iops e throughput para este tipo de volume
  - gp3: Use os parâmetros iops e throughput para este tipo de volume
  - io1: Use apenas o parâmetro iops para este tipo de volume
  - io2: Use apenas o parâmetro iops para este tipo de volume

  O tipo de volume padrão é **gp2**.
- `PersistWBC`: Controla se o disco de cache deve ser mantido ou descartado sempre que as instâncias gerenciadas do Amazon WorkSpaces Core forem desligadas. Se definido como `true`, o disco de cache é mantido. Se definido como `false` (o padrão), o disco de cache é criado e mantido apenas enquanto a instância AMI estiver ligada.
- `PersistOSDisk`: Controla se o disco do SO deve ser mantido ou descartado sempre que as instâncias gerenciadas do Amazon WorkSpaces Core forem desligadas. Se definido como `true`, o disco do SO é mantido. Se definido como `false` (o padrão), o disco do SO é criado e mantido apenas enquanto a instância AMI estiver ligada.

Execute as seguintes etapas na janela do PowerShell para criar um catálogo não persistente habilitado para MCSIO:

1. Abra a janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um catálogo de broker e um pool de identidades.

4. Crie o esquema de provisionamento. Por exemplo:

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'



$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. Adicione VMs ao catálogo.

Melhorar o desempenho de inicialização com MCSIO

Você pode melhorar o desempenho de inicialização das VMs se habilitar o MCSIO e definir as propriedades personalizadas `PersistWBC` e `PersistOSDisk` como `true`. Com essa configuração, as VMs podem inicializar mais rapidamente porque não precisam inicializar um novo disco de cache ou recriar um disco raiz a partir de seu modelo.

Criptografar discos de SO e ID

Você pode criar um catálogo de VMs com chaves AWS KMS (chave gerenciada pelo cliente e chave gerenciada pela AWS) que podem ser usadas para criptografar o disco do SO e o Disco de Identidade (ID).

- As chaves gerenciadas pela AWS são rotacionadas automaticamente todos os anos.
- As chaves gerenciadas pelo cliente são opcionais para rotação automática e podem ser gerenciadas manualmente.

Você pode consultar os seguintes documentos da AWS para obter mais informações sobre chaves KMS:

- Conceitos do AWS KMS
- Como funciona a rotação automática de chaves

Para criptografia de discos de SO e ID, configure um dos seguintes:

- Use uma imagem preparada que esteja criptografada (por exemplo, uma AMI criada a partir de uma instância ou snapshot que contém um volume raiz EBS criptografado com chave KMS)
- Use uma fonte de perfil de máquina (VM ou modelo de inicialização) que contenha um volume raiz EBS criptografado.

Limitações

Considere as seguintes limitações:

- O MCS atualmente suporta apenas um disco na AMI de imagem preparada.
- Você não pode criptografar diretamente volumes ou snapshots EBS existentes não criptografados, ou modificar a chave KMS de um volume criptografado existente. Para fazer isso, você deve:

  a. Crie um novo snapshot desse volume.

  b. Crie um novo volume a partir desse snapshot

  c. Criptografe o novo volume.

Consulte os seguintes documentos da AWS:

- Criptografar recursos não criptografados
- Limitações da criptografia automática ou padrão de volumes EBS: Criptografar automaticamente volumes Amazon EBS existentes e novos.

Criar um catálogo com criptografia de disco

Você pode criar um catálogo de máquinas MCS com criptografia de disco usando:

- Imagem preparada (criada usando o gerenciamento de imagem a partir de uma imagem mestre que possui disco criptografado)
- Perfil de máquina

As considerações ao usar a entrada do perfil da máquina são:

- A chave KMS da entrada do perfil da máquina tem precedência sobre a chave KMS da imagem preparada.
- Se nenhuma entrada de perfil de máquina for fornecida, a chave KMS da AMI da imagem preparada será usada para criptografar os discos das VMs do catálogo.
- Se o perfil da máquina tiver Mapeamentos de Dispositivo de Bloco presentes, os dispositivos de bloco presentes no modelo de imagem preparada (AMI) e no perfil da máquina devem corresponder. Por exemplo, se a AMI tiver um dispositivo definido em `/dev/sda1`, então o Perfil da Máquina também deve ter um dispositivo definido em `/dev/sda1`.
- Se não houver uma chave na origem do perfil da máquina e a imagem preparada não estiver criptografada, os discos das VMs do catálogo não serão criptografados.
- Quando a imagem preparada é criptografada, uma VM de origem de perfil de máquina ou um modelo de inicialização deve ter um volume raiz criptografado para ser considerado uma entrada válida.

Modificar um catálogo existente

Você pode modificar um catálogo existente usando o comando PowerShell `Set-ProvScheme` para ter:

- Uma entrada de perfil de máquina com um volume contendo uma nova chave KMS.
- Uma imagem preparada criada a partir da imagem mestre com AMI criptografada usando gerenciamento de imagens.

Considerações importantes:

- Os volumes das novas VMs adicionadas ao catálogo são criptografados com a nova chave KMS.
- Para atualizar as configurações de criptografia quando houver um perfil de máquina existente, execute `Set-ProvScheme` com um novo perfil de máquina.
- Você não pode modificar um catálogo existente de volumes criptografados para volumes não criptografados. Você não pode fazer uma atualização de imagem de uma AMI de imagem preparada criptografada para uma AMI de imagem preparada não criptografada.

Habilitar NitroTPM e inicialização segura UEFI para instâncias de VM

Ao criar um catálogo, agora você pode selecionar uma imagem preparada (AMI) com NitroTPM e/ou inicialização segura UEFI habilitados. Consequentemente, as VMs provisionadas no catálogo também são habilitadas com NitroTPM e/ou inicialização segura UEFI. Essa implementação garante que as VMs sejam seguras e confiáveis. Para obter mais informações sobre NitroTPM e inicialização segura UEFI, consulte a documentação da Amazon.

Limitações

- Você pode usar NitroTPM e Secure Boot atualmente em todas as regiões da AWS (incluindo as regiões AWS GovCloud (US)), exceto na China.
- Você não pode habilitar NitroTPM e inicialização segura UEFI em catálogos existentes. Se você deseja um catálogo com NitroTPM e inicialização segura UEFI habilitados, crie um novo catálogo.

Principais etapas

1. Configure seu ambiente AWS.
2. Crie uma conexão com a AWS.
3. Crie uma imagem mestre (AMI) habilitada com NitroTPM e/ou inicialização segura UEFI.
4. Crie uma imagem preparada a partir da imagem mestre. Consulte Criar uma imagem preparada para instâncias gerenciadas do Amazon WorkSpaces Core.
5. Crie um catálogo de máquinas selecionando a imagem preparada com NitroTPM e inicialização segura UEFI habilitados no menu de criação de catálogo do Citrix Studio ou ao criar um Esquema de Provisionamento usando comandos PowerShell.

As VMs adicionadas ao catálogo criado têm NitoTPM e inicialização segura UEFI habilitados.

Crie uma AMI que suporte NitroTPM e inicialização segura UEFI

1. Você pode criar uma AMI a partir de uma VM que tenha NitroTPM e/ou inicialização segura UEFI habilitados.
   a. Crie a instância usando as imagens do AWS Marketplace. Exemplo, pesquise por `TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`.
   b. Baixe o VDA de sessão única ou múltipla.
   c. Crie uma AMI a partir dessa VM.
2. Use o comando register-image:

   ```
   --boot-mode (string)

   --tpm-support (string)
   ```

   Para obter mais informações, consulte register-image.

Consulte os seguintes documentos da AWS:

- Determinar os modos de inicialização suportados de um tipo de instância EC2
- Requisitos para usar o NitroTPM com instâncias Amazon EC2/.

Você pode abrir uma janela do PowerShell a partir do host do Delivery Controller™ para verificar se um específico:

- oferta de serviço suporta NitroTPM ou inicialização segura UEFI

  ```
  (Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
  Instance.serviceoffering”).AdditionalData.BootMode

  (Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
  Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
  ```

- modelo suporta NitroTPM ou inicialização segura UEFI

  ```
  (Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
  -ResourceType “template -Id “ID”).AdditionalData.BootMode
  ```

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

Atualizar a oferta de serviço do catálogo existente

Você pode alterar a oferta de serviço de um catálogo existente usando `Set-ProvScheme`. A alteração se aplica às VMs recém-adicionadas. No entanto, você recebe erros nos seguintes cenários:

MODO DE INICIALIZAÇÃO DAS AMIS	A AMI SUPORTA NITRO TPM?	A OFERTA DE SERVIÇO SUPORTA NITROTPM E INICIALIZAÇÃO SEGURA UEFI?
UEFI	Não	Não
BIOS Legado	Sim	Não
UEFI	Sim	Não
UEFI Preferencial	Sim	Não

Copiar tags em VMs

Você pode copiar tags em NICs e discos (disco de identidade, disco de cache de write-back e disco do SO) que são especificados no perfil da máquina para VMs recém-criadas em um catálogo de máquinas MCS. Você pode especificar essas tags em qualquer uma das fontes de perfil da máquina (instância de VM AWS ou versão de modelo de inicialização AWS). Esse recurso é aplicável a catálogos de máquinas e VMs persistentes e não persistentes.

Nota:

- No console do AWS EC2, você não pode ver os valores de **Tag Network Interfaces** em **Launch Template Version Resource Tags**. No entanto, você pode executar o comando PowerShell `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` para ver as especificações da tag.

- Se uma fonte de perfil de máquina (VM ou versão de modelo de inicialização) tiver duas interfaces de rede (eni-1 e eni-2), e eni-1 tiver a tag t1 e eni-2 tiver a tag t2, então a VM receberá as tags de ambas as interfaces de rede.

Filtrar instâncias de VM usando PowerShell

Uma instância de VM AWS que você usa como VM de perfil de máquina deve ser compatível para que o catálogo de máquinas seja criado e funcione corretamente. Para listar as instâncias de VM AWS que podem ser usadas como VMs de entrada de perfil de máquina, você pode usar o comando `Get-HypInventoryItem`. O comando pode paginar e filtrar o inventário de VMs disponíveis em uma unidade de hospedagem.

Paginação:

Get-HypInventoryItem suporta dois modos de paginação:

- O modo de paginação usa os parâmetros `-MaxRecords` e `-Skip` para retornar conjuntos de itens:
  - `-MaxRecords`: O padrão é **1**. Isso controla quantos itens retornar.
  - `-Skip`: O padrão é **0**. Isso controla quantos itens pular desde o início absoluto (ou fim absoluto) da lista no hipervisor.
- O modo de rolagem usa os parâmetros `-MaxRecords`, `-ForwardDirection` e `-ContinuationToken` para permitir a rolagem dos registros:
  - `-ForwardDirection`: O padrão é **True**. Isso é usado junto com `-MaxRecords` para retornar o próximo conjunto de registros correspondentes ou o conjunto anterior de registros correspondentes.
  - `-ContinuationToken`: Retorna os itens imediatamente após (ou antes, se `ForwardDirection` for **false**) mas não incluindo o item fornecido em `ContinuationToken`.

Exemplos de paginação:

- Para retornar um único registro do modelo de máquina com o nome mais baixo. O campo `AdditionalData` tem o `TotalItemsCount` e o `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- Para retornar 10 registros do modelo de máquina com o nome mais baixo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- Para retornar um array de registros terminando com o nome mais alto:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- Para retornar um array de registros começando no modelo de máquina associado ao `ContinuationToken` fornecido:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

Filtragem:

Os seguintes parâmetros opcionais adicionais são suportados para filtragem. Você pode combinar esses parâmetros com as opções de paginação.

- `-ContainsName "my_name"`: Se a string fornecida corresponder a parte de um nome de AMI, a AMI será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: Se uma AMI tiver pelo menos uma dessas tags, ela será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

Nota:

Dois valores de tag são suportados. O valor de tag **Não Marcado** corresponde a itens que não possuem a tag fornecida em sua lista de tags. O valor de tag **Todos os valores** corresponde a itens que possuem a tag, independentemente do valor da tag. Caso contrário, a correspondência ocorre apenas se o item tiver a tag e o valor for igual ao que é fornecido no filtro.

- `-Id "ami-0a2d913927e0352f3"`: Se a AMI corresponder ao ID fornecido, ela será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

Filtragem no parâmetro AdditionalData:

O parâmetro de filtro `AdditionalData` lista modelos ou VMs com base em sua capacidade, oferta de serviço ou qualquer propriedade que esteja em AdditionalData. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

Você também pode adicionar um parâmetro `-Warn` para indicar as VMs incompatíveis. As VMs são incluídas com um campo `AdditionalData` chamado **Aviso**. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxxx"
-Warn $true).AdditionalData
```

Onde ir em seguida

- Para gerenciar um catálogo do Amazon Workspaces Core, consulte Gerenciar um catálogo de instâncias gerenciadas do Amazon WorkSpaces Core

Mais informações

- Ambientes de virtualização AWS
- Conexão com instâncias gerenciadas do Amazon WorkSpaces Core
- Gerenciamento de imagens
- Criar uma imagem preparada para instâncias gerenciadas do Amazon WorkSpaces Core
- Para exemplos de PowerShell do GitHub do Amazon WorkSpaces Core, consulte citrix-mcs-sdk-samples-Amazon WorkSpaces Core.

Criar um catálogo de máquinas Amulet Hotkey CoreStation

Criar catálogos de máquinas descreve o fluxo de trabalho genérico do catálogo de máquinas. As informações a seguir cobrem detalhes específicos do Amulet Hotkey CoreStation.

> **Nota:**
>
> - Antes de criar um catálogo Amulet Hotkey CoreStation, conclua Conexão com Amulet Hotkey CoreStation.
> - Certifique-se de ter um ou mais nós Amulet Hotkey CoreStation disponíveis e instale VDAs nesses nós.
> - Para obter informações sobre como criar a imagem inicial do cartucho Amulet Hotkey CoreStation, consulte o Guia do Usuário de Implantação de SO no CoreStation.

Você pode criar um catálogo de máquinas Amulet Hotkey CoreStation usando:

- Studio
- Comandos PowerShell

Usando o Studio

No assistente de Configuração do Catálogo de Máquinas:

1. Na página **Sistema Operacional**, selecione **SO multissessão** ou **SO de sessão única**.
2. Na página **Gerenciamento de Máquinas**, selecione **Máquinas com gerenciamento de energia e Outro serviço ou tecnologia**.
3. Na página **Máquinas Virtuais**, adicione máquinas e suas contas de máquina do Active Directory. Você pode fazer uma das seguintes opções:

- Clique em **Adicionar Máquinas** para adicionar máquinas manualmente. A janela **Selecionar VMs** é exibida. Expanda a conexão do gabinete Amulet Hotkey CoreStation que você criou anteriormente e selecione os nós que deseja adicionar. Em seguida, adicione os nomes das contas de máquina associadas.
- Clique em **Adicionar Arquivo CSV** para adicionar máquinas em massa. Para obter informações sobre como usar arquivos CSV para adicionar máquinas, consulte Usar arquivos CSV para adicionar máquinas em massa a um catálogo.

As páginas **Escopos** e **Resumo** não contêm informações específicas do Amulet Hotkey CoreStation.

Usando comandos PowerShell

Execute os comandos PowerShell `New-BrokerCatalog` e `New-BrokerMachine` para criar um catálogo de broker e importar máquinas para o catálogo de broker.

Por exemplo:

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

Onde ir em seguida

- Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.
- Para revisar todo o processo de configuração, consulte Planejar e construir uma implantação.
- Para gerenciar energia, consulte Gerenciar energia de VMs Amulet Hotkey CoreStation.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com Amulet Hotkey CoreStation
- Criar catálogos de máquinas

Criar um catálogo AWS EC2

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização AWS EC2.

> **Nota:**
>
> Antes de criar um catálogo AWS, você precisa concluir a criação de uma conexão com a AWS. Consulte Conexão com AWS EC2.

Configuração de rede durante a preparação da imagem

Durante a preparação da imagem, uma máquina virtual (VM) de preparação é criada com base na VM original. Esta VM de preparação é desconectada da rede. Para desconectar a rede da VM de preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e saída. Este grupo de segurança de rede persiste e é reutilizado. O nome do grupo de segurança de rede é `Citrix.XenDesktop.IsolationGroup-GUID`, onde GUID é gerado aleatoriamente.

Tenancy da AWS

A AWS oferece as seguintes opções de tenancy:

- Tenancy compartilhada (o tipo padrão) e tenancy dedicada. Tenancy compartilhada significa que várias instâncias do Amazon EC2 de diferentes clientes podem residir na mesma peça de hardware físico.
- Tenancy dedicada significa que suas instâncias EC2 são executadas apenas em hardware com outras instâncias que você implantou. Outros clientes não usam a mesma peça de hardware.

Requisitos para provisionamento em hosts AWS

- Uma imagem BYOL (traga sua própria licença) importada (AMI). Com hosts dedicados, use e gerencie suas licenças existentes.
- Uma alocação de hosts dedicados com utilização suficiente para satisfazer as solicitações de provisionamento.
- Habilitar o **auto-placement**.

Opções para configurar a tenancy da AWS

- **Usar hardware compartilhado**. Esta configuração é adequada para a maioria das implantações. Vários clientes compartilham partes do hardware, embora não interajam entre

si. Usar hardware compartilhado é a opção menos dispendiosa para executar suas instâncias do Amazon EC2.

- **Usar host dedicado**. Um host dedicado do Amazon EC2 é um servidor físico com capacidade de instância EC2 totalmente dedicada, permitindo que você use licenças de software existentes por soquete ou por VM. Hosts dedicados têm utilização predefinida com base no tipo de instância. Por exemplo, um único host dedicado alocado de tipos de instância C4 Large é limitado a executar 16 instâncias. Consulte o site da AWS para obter mais informações.

  Esta configuração é adequada para implantações com restrições de licenciamento ou requisitos de segurança que exigem o uso de um host dedicado. Com um host dedicado, você possui um host físico inteiro e é cobrado por hora. Possuir esse host permite que você crie quantas instâncias EC2 o host permitir, sem custos adicionais.

- **Usar instância dedicada**. Esta configuração é mais adequada para implantações com requisitos específicos de segurança ou conformidade. Com uma instância dedicada, você ainda desfruta dos benefícios de ter um host separado de outros clientes AWS, mas não paga pelo host inteiro. Você não precisa se preocupar com a capacidade do host, mas é cobrado a uma taxa mais alta pelas instâncias.

> **Nota:**
>
> Você pode excluir qualquer disco de identidade de preparação disponível se não houver uma tarefa de criação de catálogo ou atualização de imagem em andamento.

> Para configurar a tenancy da AWS usando o Studio, consulte Criar um catálogo usando o Studio e, usando o PowerShell, consulte Configurar a tenancy de host dedicado da AWS usando o PowerShell.

Marcar recursos operacionais da AWS

Uma Amazon Machine Image (AMI) representa um tipo de appliance virtual usado para criar uma máquina virtual dentro do ambiente Amazon Cloud, comumente referido como EC2. Você usa uma AMI para implantar serviços que usam o ambiente EC2. Ao criar um catálogo para provisionar máquinas usando o MCS para AWS, você seleciona a **AMI** para atuar como a imagem dourada para esse catálogo.

> **Importante:**

> A criação de catálogos usando um perfil de máquina e um modelo de inicialização é necessária para usar a marcação de recursos operacionais.

> Para criar um catálogo AWS, você deve primeiro criar uma AMI para a instância que deseja que seja a imagem dourada. O MCS lê as tags dessa instância e as incorpora no modelo de inicialização. As tags do modelo de inicialização são então aplicadas a todos os recursos Citrix® criados em seu ambiente AWS, incluindo:

- Máquinas Virtuais
- Discos de VM
- Interfaces de rede de VM
- Buckets S3
- Objetos S3
- Modelos de inicialização
- AMIs

Você pode marcar recursos operacionais usando o Studio e o PowerShell ao criar um catálogo. Para o Studio, consulte Criar um catálogo usando o Studio (página **Imagem**). Para o PowerShell, consulte Marcar recursos operacionais usando o PowerShell.

Criar um catálogo

Você pode criar um catálogo usando:

- Studio
- PowerShell

Criar um catálogo usando o Studio

1. Clique em **Catálogos de Máquinas** no painel de navegação esquerdo.
2. Clique em **Criar Catálogo de Máquinas**. A página **Configuração do Catálogo de Máquinas** é exibida.
3. Na página **Tipo de Máquina**, selecione um tipo de máquina para o catálogo, por exemplo, SO multissessão.
4. Na página **Gerenciamento de Máquinas**, selecione as seguintes configurações:

    a. Selecione Máquinas que têm gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade).

b. Selecione **Tecnologia de provisionamento Citrix**. Em seguida, selecione **Citrix Machine Creation Services™**.

c. No campo **Recursos**, selecione os recursos (Zona de Disponibilidade ou Zona Local) que você configurou ao criar a conexão do host e clique em **Avançar**.

5. Na página **Experiência da área de trabalho**, selecione a área de trabalho aleatória ou estática que você deseja que os usuários tenham ao fazer login.
6. Na página **Imagem**:

a. Selecione um modelo de máquina que você deseja usar como imagem mestre para todas as máquinas no catálogo.

b. Se você quiser que as VMs no catálogo herdem as configurações de um perfil de máquina, selecione um perfil de máquina. Por padrão, a caixa de seleção **Usar um perfil de máquina** está selecionada. Para alterar a origem do perfil de máquina para outra VM ou versão de modelo de inicialização, clique no botão editar.

c. Se o modelo de máquina tiver dois volumes, a opção **Provisionar um disco de dados** será habilitada por padrão. Nesse caso, os perfis de máquina são filtrados apenas com as instâncias ou modelos de inicialização com dois volumes (que especificam as propriedades de hardware, por exemplo, mapeamento de dispositivo de bloco, tipo de volume) para os dois volumes, e modelos de inicialização sem volumes e mapeamentos de dispositivo de bloco definidos.

Se você desmarcar a caixa de seleção para provisionar um disco de dados, os perfis de máquina serão filtrados apenas com os modelos de inicialização sem volumes e mapeamentos de dispositivo de bloco definidos.

Para um catálogo MCS baseado em perfil de máquina, você pode usar a mesma VM mestre como origem do disco de dados para o perfil de máquina.

d. Marque a caixa de seleção **Aplicar tags de máquina a recursos operacionais** para aplicar tags de máquina a recursos operacionais. Essa opção controla se as tags de máquina devem ser aplicadas a cada item criado em seu ambiente AWS que facilita o provisionamento de máquinas. Os recursos operacionais são criados como subprodutos da criação do catálogo. Eles incluem recursos temporários e persistentes, como instâncias de VM de preparação e AMI.

> **Nota:**

> A página **Segurança** aparece somente se você estiver criando um catálogo de máquinas sem atribuir um perfil de máquina.

7. Na página **Máquinas Virtuais**:
   a. Insira o número de VMs para o catálogo.
   b. A especificação de máquina padrão é exibida, que é baseada no perfil de máquina. Para alterá-la, selecione o ícone de edição e selecione uma especificação de máquina.
   c. Configure a tenência AWS. Consulte Opções para configurar a tenência AWS.
   d. Você também pode configurar uma VM secundária quando o tamanho da máquina primária atingir a capacidade total. Clique em **Tamanho secundário** (opcional). Na janela **Tamanho da máquina secundária**, as VMs listadas têm tipos de VM Spot e Regular. Você pode selecionar até 10 tamanhos de máquina secundária. Depois que as 10 VMs forem selecionadas, as outras VMs listadas serão desabilitadas para seleção futura. Clique em **Avançar**. No painel **Tamanho da máquina secundária**, você pode selecionar vários tamanhos de máquina e arrastar e soltar para alterar a ordem de prioridade. Clique em **Concluído**. Os tamanhos de máquina selecionados aparecem em Tamanho secundário (opcional). Clique no ícone de edição para editar conforme necessário.
8. A página **Segurança** aparece somente se você estiver criando um catálogo de máquinas sem atribuir um perfil de máquina. Use a página **Segurança** para configurar os grupos de segurança para as VMs. Isso também é aplicável ao editar e clonar um catálogo de máquinas existente.

   Se você criar um catálogo de máquinas baseado em perfil de máquina, as configurações do grupo de segurança serão herdadas do perfil de máquina e a página **Segurança** não aparecerá.
9. Na página **NICs**, selecione as NICs (ou ENIs) para as VMs.
10. Na página **Configurações de Disco**, escolha se deseja habilitar o cache de write-back.
11. Na página **Identidades da Máquina**, configure o Active Directory local ou o Microsoft Entra híbrido para as máquinas no catálogo, selecionando o domínio e criando novas contas AD para as VMs a serem criadas neste catálogo de máquinas. As VMs provisionadas são unidas ao domínio selecionado. Especifique o esquema de nomenclatura de conta para as novas contas AD a serem criadas para as VMs. Clique em Avançar.
12. Na página **Credenciais de domínio**, clique em **Inserir credenciais** para fornecer as credenciais para o domínio selecionado. Insira o nome de usuário e a senha de nível de

administrador quando solicitado. Você também pode usar uma conta de serviço se já tiver credenciais de domínio salvas anteriormente, seguindo a documentação do nosso produto.

13. Avance pelas páginas restantes até a página **Resumo**. Se você selecionar para provisionar um disco de dados na página **Imagens**, o valor de **Usar disco de dados** será definido como **true** na página **Resumo**. Insira um nome para o catálogo de máquinas e selecione **Concluir** para criar o catálogo de máquinas.

Limitações na criação de um catálogo de máquinas em uma zona local da AWS

- Certas zonas locais suportam apenas certas configurações de hardware (por exemplo, a zona local de Perth não suporta volumes GP3, apenas GP2).
- Como apenas gp2 é universalmente suportado em todas as zonas locais, e nem todas suportam gp3, a criação de disco de ID padroniza o uso do tipo de volume gp2.
- Você deve selecionar um perfil de máquina com especificações de hardware que sejam suportadas na zona local desejada.
- Os snapshots de AMIs de imagem preparada e os snapshots de disco de ID são padronizados para serem colocados na região, em vez da zona local (devido às limitações da AWS em relação à visibilidade do suporte a snapshots EBS em zonas locais).
- Apenas zonas locais que suportam serviços EC2 e EBS completos são zonas suportadas.

Criar um catálogo usando PowerShell

Configurar a locação de host dedicado AWS usando o PowerShell

Alternativamente, você pode provisionar hosts dedicados AWS através do PowerShell. Use o cmdlet `New-ProvScheme` com o parâmetro `TenancyType` definido como `Host`.

Marcar recursos operacionais usando PowerShell

Para usar o PowerShell para marcar recursos:

1. Abra uma janela do PowerShell a partir do host DDC.
2. Execute o comando `asnp citrix` para carregar módulos PowerShell específicos da Citrix.

Para marcar um recurso para uma VM provisionada, use a propriedade personalizada `AwsOperationalResourcesTagging`. Exemplo:

```
New-ProvScheme -ProvisioningSchemeName test

-CustomProperties “AwsOperationalResourcesTagging,true”
```

```
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"

... <Other <standard provscheme parameters>
```

Catálogo habilitado para MCSIO

A Otimização de Armazenamento MCS (MCSIO) melhora o desempenho da VM armazenando em cache as operações de disco na memória ou em um disco pequeno de alta velocidade. Você pode criar um catálogo não persistente habilitado para MCSIO usando comandos PowerShell. Para criar tal catálogo, você deve instalar o driver MCSIO durante a instalação ou atualização do VDA, durante a preparação da instância AMI. Por padrão, esse driver não é instalado.

Depois que uma AMI MCSIO é preparada (ao instalar o VDA, selecione a opção para incluir o driver MCSIO na instalação), você pode criar um catálogo não persistente habilitado para MCSIO.

Nota:

A opção de configurar o MCSIO apenas com cache de disco (sem cache de memória) usando o Studio foi removida em todos os hipervisores e ambientes de serviço em nuvem.

Criar um catálogo habilitado para MCSIO

Os quatro parâmetros adicionados ao comando PowerShell New-ProvScheme são:

- `UseWriteBackCache`: Ativa o cache (cache de write-back) para o esquema de provisionamento fornecido
- `WriteBackCacheDiskSize`: Especifica o tamanho em GB do disco temporário usado para cache
- `WriteBackCacheMemorySize`: Especifica a quantidade de memória em MB a ser usada para cache. Este é um parâmetro opcional.

Nota:

> - O valor de `WriteBackCacheDiskSize` deve ser maior que zero porque é necessário pelo menos 1 GB de armazenamento em disco de cache. O tamanho do disco de cache não deve ser maior que o tamanho do disco do SO.
> - O valor de `WriteBackCacheMemorySize` deve ser diferente de zero e menor que o tamanho da memória do catálogo de máquinas.

> As propriedades personalizadas que afetam o MCSIO são:

- `WBCDiskStorageType`: Define o tipo de volume, que é usado para o disco temporário no AWS. Este parâmetro aceita um argumento de string no formato `volume-type[:iops][:throughput]`. Os seguintes são os tipos de volume:
  - gp2: Não use os parâmetros iops e throughput para este tipo de volume
  - gp3: Use os parâmetros iops e throughput para este tipo de volume
  - io1: Use apenas o parâmetro iops para este tipo de volume
  - io2: Use apenas o parâmetro iops para este tipo de volume

  O tipo de volume padrão é **gp2**.
- `PersistWBC`: Controla se o disco de cache deve ser mantido ou descartado sempre que a instância AWS é desligada. Se definido como `true`, o disco de cache é mantido. Se definido como `false` (o padrão), o disco de cache é criado e mantido apenas enquanto a instância AMI estiver ligada.
- `PersistOSDisk`: Controla se o disco do SO deve ser mantido ou descartado sempre que a instância AWS é desligada. Se definido como `true`, o disco do SO é mantido. Se definido como `false` (o padrão), o disco do SO é criado e mantido apenas enquanto a instância AMI estiver ligada.

Execute os seguintes passos na janela do PowerShell para criar um catálogo não persistente com MCSIO habilitado:

1. Abra a janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um catálogo de broker e um pool de identidades.
4. Crie o esquema de provisionamento. Por exemplo:

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'




$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. Adicione VMs ao catálogo.

Melhore o desempenho de inicialização com MCSIO

Você pode melhorar o desempenho de inicialização das VMs se habilitar o MCSIO e definir as propriedades personalizadas `PersistWBC` e `PersistOSDisk` como `tru`. Com essa configuração, as VMs podem inicializar mais rapidamente porque não precisam inicializar um novo disco de cache ou recriar um disco raiz a partir de seu modelo.

Crie um catálogo de máquinas baseado em perfil de máquina usando PowerShell

Você pode usar um perfil de máquina para capturar as propriedades de hardware de uma instância EC2 (VM) ou versão de modelo de inicialização e aplicá-las às máquinas provisionadas. As propriedades capturadas podem incluir, por exemplo, propriedades de volume EBS, tipo de instância, otimização EBS, opções de CPU, tipo de locação, capacidade de hibernação, grupos de segurança e outras configurações AWS suportadas.

Você pode usar uma instância AWS EC2 (VM) ou uma versão de modelo de inicialização AWS como entrada do perfil da máquina.

> **Nota:**
>
> As propriedades do volume EBS são derivadas apenas de um perfil de máquina.

Considerações importantes

As considerações importantes ao criar um catálogo de máquinas MCS:

- Se você adicionar parâmetros de propriedade de hardware da máquina nos comandos `New-ProvScheme` e `Set-ProvScheme`, os valores fornecidos nos parâmetros sobrescreverão os valores no perfil da máquina.
- Se você definir `AwsCaptureInstanceProperties` como `true` e não definir a propriedade `MachineProfile`, então apenas as funções e tags do IAM serão capturadas.
- Você não pode definir `AwsCaptureInstanceProperties` e `MachineProfile` ao mesmo tempo.

  > **Nota:**
  >
  > O `AwsCaptureInstanceProperties` está obsoleto.

- Se um perfil de máquina não for fornecido, você deve fornecer explicitamente os valores das seguintes propriedades:
  - Grupo de Segurança
  - ENI ou Rede Virtual
- Você pode habilitar `AwsOperationalResourcesTagging` somente se habilitar `AwsCaptureInstanceProperties` ou especificar um perfil de máquina.

A consideração importante após criar um catálogo de máquinas MCS é:

- Você não pode alterar um catálogo de baseado em perfil de máquina para um catálogo não baseado em perfil de máquina.

Configurar grupos de segurança em uma entrada de perfil de máquina

Você pode criar um catálogo de máquinas MCS onde as VMs provisionadas recebem grupos de segurança por ENI (Interface de Rede). Para fazer isso, use uma entrada de perfil de máquina (instância EC2 ou modelo de inicialização) que tenha diferentes grupos de segurança mapeados para ENIs distintas. Por exemplo, se a entrada do perfil da máquina tiver ENI A com SG 1 e ENI B com SG 2, então as VMs provisionadas também devem ter ENI A com SG 1 e ENI B com SG 2.

Recuperar detalhes da interface de rede

Execute os seguintes comandos para obter a lista de registros de dados da interface de rede, incluindo o SubnetId da interface, grupos de segurança atribuídos e redes atribuídas.

```
(Get-HypInventoryItem -LiteralPath 'XdHyp:\HostingUnits\cvad-test' –
ResourceType vm). AdditionalData
```

> **Nota:**
>
> O MCS atualmente não permite mais de uma rede por interface de rede.

Criar um catálogo de máquinas usando um perfil de máquina

Para criar um catálogo de máquinas usando um perfil de máquina:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um pool de identidades, se ainda não tiver sido criado. Por exemplo,

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. Execute o comando New-ProvScheme. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. Conclua a criação do catálogo.

Atualizar o perfil da máquina

Para atualizar o perfil da máquina em um catálogo que foi inicialmente provisionado com um perfil de máquina, faça o seguinte. Você também pode alterar o tipo de locação e a capacidade de hibernação da origem do perfil da máquina ao editar um catálogo de máquinas MCS.

1. Execute o comando `Set-ProvScheme`. Por exemplo,

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

Criar um catálogo com a versão do modelo de inicialização usando o PowerShell

Você pode criar um catálogo de máquinas MCS com uma versão de modelo de inicialização como entrada de perfil de máquina. Você também pode atualizar a entrada de um catálogo de perfil de

máquina de uma VM para uma versão de modelo de inicialização e de uma versão de modelo de inicialização para uma VM.

No console do AWS EC2, você pode fornecer as informações de configuração da instância de um modelo de inicialização junto com o número da versão. Ao especificar a versão do modelo de inicialização como entrada de perfil de máquina ao criar ou atualizar um catálogo de máquinas, as propriedades dessa versão do modelo de inicialização são copiadas para as VMs VDA provisionadas.

As seguintes propriedades podem ser fornecidas usando a entrada do perfil da máquina ou explicitamente como parâmetros nos comandos `New-ProvScheme` ou `Set-ProvScheme`. Se forem fornecidas nos comandos `New-ProvScheme` ou `Set-ProvScheme`, elas terão precedência sobre os valores do perfil da máquina dessas propriedades.

- Oferta de Serviço
- Redes
- Tipo de Tenancy

> **Nota:**
>
> Se a oferta de serviço não for fornecida no modelo de inicialização do perfil da máquina ou como um parâmetro no comando `New-ProvScheme`, você receberá um erro apropriado.

> Para criar um catálogo usando a versão do modelo de inicialização como entrada de perfil da máquina:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Obtenha a lista de versões do modelo de inicialização de um modelo de inicialização. Por exemplo:

   ```
   XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
   Select FullPath
   ```

4. Crie um pool de identidades, se ainda não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. Crie um esquema de provisionamento com uma versão do modelo de inicialização como entrada de perfil da máquina. Por exemplo:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. Registre um esquema de provisionamento como um catálogo de broker. Por exemplo:

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
```

```
-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. Conclua a criação do catálogo.

Atualizar a origem do perfil da máquina

Você também pode atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização e de uma versão de modelo de inicialização para uma VM. Por exemplo:

- Para atualizar a entrada de um catálogo de perfil de máquina de uma VM para uma versão de modelo de inicialização:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- Para atualizar a entrada de um catálogo de perfil de máquina de uma versão de modelo de inicialização para uma VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

Criptografar discos de SO, ID e WBC

Você pode criar um catálogo persistente e não persistente de VMs com chaves AWS KMS (chave gerenciada pelo cliente e chave gerenciada pela AWS) que podem ser usadas para criptografar disco do SO, disco de identidade (ID) e disco de cache de write-back (WBC).

- As chaves gerenciadas pela AWS são rotacionadas automaticamente todos os anos.

- As chaves gerenciadas pelo cliente são opcionais para rotação automática e podem ser gerenciadas manualmente.

Você pode consultar os seguintes documentos da AWS para obter mais informações sobre chaves KMS:

- Conceitos do AWS KMS
- Como funciona a rotação automática de chaves

Para criptografia de discos de SO, ID e WBC, configure um dos seguintes:

- Use uma imagem mestre criptografada (por exemplo, uma AMI criada a partir de uma instância ou snapshot que contém um volume raiz EBS criptografado com chave KMS)
- Use uma fonte de perfil de máquina (VM ou modelo de inicialização) que contenha um volume raiz EBS criptografado.

Limitações

Considere as seguintes limitações:

- Atualmente, o MCS suporta apenas um disco na AMI da imagem mestre.
- Você não pode criptografar diretamente volumes ou snapshots EBS existentes não criptografados, nem modificar a chave KMS de um volume criptografado existente. Para fazer isso, você deve:

  a. Criar um novo snapshot desse volume.

  b. Criar um novo volume a partir desse snapshot

  c. Criptografar o novo volume.

Consulte os seguintes documentos da AWS:

- Criptografar recursos não criptografados
- Limitações da criptografia automática ou padrão de volumes EBS: Criptografar automaticamente volumes EBS existentes e novos da Amazon.

Criar um catálogo com criptografia de disco

Você pode criar um catálogo de máquinas MCS com criptografia de disco usando:

- Imagem mestre
- Perfil da máquina

As considerações ao usar a entrada do perfil da máquina são:

- A chave KMS da entrada do perfil da máquina tem precedência sobre a chave KMS da imagem mestre.
- Se nenhuma entrada de perfil de máquina for fornecida, a chave KMS da AMI da imagem mestre será usada para criptografar os discos das VMs do catálogo.
- Se o perfil da máquina tiver Mapeamentos de Dispositivo de Bloco presentes, então os dispositivos de bloco presentes no modelo de imagem mestre (AMI) e no perfil da máquina devem corresponder. Por exemplo, se a AMI tiver um dispositivo definido em `/dev/sda1`, então o Perfil da Máquina também deve ter um dispositivo definido em `/dev/sda1`.
- Se não houver chave na origem do perfil da máquina e a imagem mestre não for criptografada, os discos das VMs do catálogo não serão criptografados.
- Quando a imagem mestre é criptografada, uma VM de origem de perfil de máquina ou um modelo de inicialização deve ter um volume raiz criptografado para ser considerado uma entrada válida.

Modificar um catálogo existente

Você pode modificar um catálogo existente usando o comando PowerShell `Set-ProvScheme` para ter:

- Uma entrada de perfil de máquina com um volume contendo uma nova chave KMS.
- Um modelo de imagem mestre AMI criptografado com uma nova chave KMS.

Considerações importantes:

- Os volumes das novas VMs adicionadas ao catálogo são criptografados com a nova chave KMS.
- Para atualizar as configurações de criptografia quando houver um perfil de máquina existente, execute `Set-ProvScheme` com um novo perfil de máquina.
- Você não pode modificar um catálogo existente de volumes criptografados para volumes não criptografados. Você não pode fazer uma atualização de imagem de uma AMI mestre criptografada para uma AMI mestre não criptografada.

Habilitar NitroTPM e inicialização segura UEFI para instâncias de VM

Ao criar um catálogo, agora você pode selecionar uma imagem mestre (AMI) com NitroTPM e/ou inicialização segura UEFI habilitados. Consequentemente, as VMs provisionadas no catálogo também são habilitadas com NitroTPM e/ou inicialização segura UEFI. Essa implementação

garante que as VMs sejam seguras e confiáveis. Para obter mais informações sobre NitroTPM e Inicialização Segura UEFI, consulte a documentação da Amazon.

Limitações

- Você pode usar NitroTPM e Inicialização Segura atualmente em todas as regiões da AWS (incluindo as regiões AWS GovCloud (US)), exceto na China.
- Você não pode habilitar o NitroTPM e a inicialização segura UEFI em catálogos existentes. Se você deseja um catálogo com NitroTPM e inicialização segura UEFI habilitados, crie um novo catálogo.

Etapas principais

1. Configure seu ambiente AWS.
2. Crie uma conexão com a AWS.
3. Crie uma imagem mestre (AMI) habilitada com NitroTPM e/ou inicialização segura UEFI.
4. Crie um catálogo de máquinas selecionando a imagem mestre com NitroTPM e inicialização segura UEFI habilitados no menu de criação de catálogo do Web Studio ou ao criar um Esquema de Provisionamento usando comandos PowerShell.

As VMs adicionadas ao catálogo criado têm NitoTPM e inicialização segura UEFI habilitados.

Crie uma AMI que suporte NitroTPM e inicialização segura UEFI

1. Você pode criar uma AMI a partir de uma VM que tenha NitroTPM e/ou inicialização segura UEFI habilitados.

    a. Crie a instância usando as imagens do marketplace da AWS. Exemplo, pesquise por `TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`.

    b. Baixe o VDA de sessão única ou múltipla.

    c. Crie uma AMI a partir dessa VM.

2. Use o comando register-image:

    ```
    --boot-mode (string)

    --tpm-support (string)
    ```

    Para obter mais informações, consulte register-image.

Consulte os seguintes documentos da AWS:

- Determine os modos de inicialização suportados de um tipo de instância EC2
- Requisitos para usar o NitroTPM com instâncias Amazon EC2/.

Você pode abrir uma janela do PowerShell no host do Delivery Controller™ para verificar se um específico:

- oferta de serviço suporta NitroTPM ou inicialização segura UEFI

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- modelo suporta NitroTPM ou inicialização segura UEFI

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

Atualizar a oferta de serviço do catálogo existente

Você pode alterar a oferta de serviço de um catálogo existente usando `Set-ProvScheme`. A alteração se aplica às VMs recém-adicionadas. No entanto, você recebe erros nos seguintes cenários:

MODO DE INICIALIZAÇÃO DAS AMIS	A AMI SUPORTA NITRO TPM?	A OFERTA DE SERVIÇO SUPORTA NITROTPM E INICIALIZAÇÃO SEGURA UEFI?
UEFI	Não	Não
BIOS Legado	Sim	Não
UEFI	Sim	Não
UEFI Preferencial	Sim	Não

Provisionar um disco de dados em uma VM criada pelo MCS

Um disco de dados permite o armazenamento de dados persistentes, como logs de eventos, rastreamentos de segurança e dados de aplicativos.

Você pode criar e atribuir um disco de dados persistente a uma VM persistente ou não persistente criada pelo MCS de um catálogo de máquinas MCS na AWS.

Você pode provisionar discos de dados persistentes com os discos de SO e ID. E a origem do disco de dados deve ser a imagem mestre (volume secundário da AMI).

Você pode criar catálogos MCS baseados em perfil de máquina e não baseados em perfil de máquina. Para catálogos MCS baseados em perfil de máquina, você pode usar a mesma VM de imagem mestre como a origem do disco de dados para o perfil de máquina.

Propriedades do disco de dados

O disco de dados da VM provisionada deriva:

- Tamanho e nome do dispositivo da AMI
- Tipo de volume da AMI se o perfil da máquina não for fornecido

Para catálogo baseado em perfil de máquina,

- Se o disco de dados estiver no modelo de perfil da máquina, a VM provisionada deriva as propriedades do disco de dados, como tag, política de armazenamento e camada de armazenamento, do perfil da máquina.
- O modelo de perfil da máquina também deve ter um disco de dados no mesmo índice de dispositivo que o disco de dados da AMI

Para catálogo não baseado em perfil de máquina, as informações de hardware são derivadas da AMI da imagem mestre.

O disco de dados também é criptografado com uma chave KMS e herda a chave KMS do disco de dados da AMI ou do perfil da máquina, se a chave KMS for fornecida. No entanto, o KMS do perfil da máquina tem precedência. Não é possível alterar o KMS do disco de dados.

Limitações

As seguintes operações não são atualmente suportadas:

- Provisionamento de discos de dados não persistentes.
- Usando um perfil de máquina:

    - sem disco de dados quando a AMI possui um, ou
    - em um índice de disco de dados diferente do da AMI
- Marcação por disco no momento da criação da instância.
- Restrições de nome de dispositivo de disco de dados:
    - Para AMIs do Windows, coloque o disco de dados em xvd e não em xvd
    - Para AMIs Linux, coloque o disco de dados em /dev/sd e não em /dev/sd
- Modificar catálogos e VMs existentes para usar discos de dados.
- Redefinição do disco de dados.
- Atualizar uma imagem, de um catálogo existente, que possui um disco de dados com uma imagem que não possui um disco de dados. Somente as novas VMs são atualizadas com o conteúdo da imagem e as propriedades do volume, enquanto as VMs existentes não são atualizadas.
- Provisionamento de disco WBC com disco de dados.

Criar um catálogo com disco de dados

Você pode criar um catálogo com disco de dados usando o Studio e o PowerShell.

Para o Studio, consulte Criar um catálogo usando o Studio. Além disso, consulte os seguintes pontos importantes:

- Crie uma imagem mestre (AMI) a partir de uma VM mestre com dois volumes, um do disco do SO (volume raiz) e outro para o disco de dados (volume secundário).
- Para um catálogo MCS baseado em perfil de máquina, você pode usar a mesma VM mestre como a origem do disco de dados para o perfil de máquina.
- Durante a criação do catálogo na interface do usuário do Studio, selecione a AMI que você criou com dois volumes como a imagem mestre
- A opção **Provisionar disco de dados** está habilitada por padrão.
- Selecione um perfil de máquina com 2 volumes (instância ou modelo de inicialização) ou 0 volumes (somente modelos de inicialização) que especifique as propriedades de hardware (por exemplo, mapeamento de dispositivo de bloco, tipo de volume) para os dois volumes.
- Você não pode provisionar um disco de dados quando a imagem mestre (AMI) tem:

  - Um volume: Neste caso, os perfis de máquina são filtrados apenas com as instâncias ou modelos de inicialização com 1 volume, e modelos de inicialização sem volumes e mapeamentos de dispositivo de bloco definidos.
  - Mais de 2 volumes: Neste caso, os perfis de máquina são filtrados com apenas os modelos de inicialização sem volumes e mapeamentos de dispositivos de bloco definidos

- Conclua a criação do catálogo e o disco de dados será provisionado para as VMs no catálogo

Usar o SDK do PowerShell

1. Crie uma imagem mestre (AMI) a partir de uma VM mestre com um disco de dados na AWS.

   Para um catálogo MCS baseado em perfil de máquina, você pode usar a mesma VM mestre como a origem do disco de dados para o perfil de máquina.

2. Crie um catálogo de máquinas MCS com VMs provisionadas com disco de dados usando o comando PowerShell `New-ProvScheme` com o valor do parâmetro `DataDiskPersistence` - `"Persistent"`. Por exemplo:

   ```
   New-ProvScheme  -CleanOnBoot -HostingUnitName "<HostingUnitName >"
   -IdentityPoolName "<IdentityPoolName >" -InitialBatchSizeHint 1
   -MasterImageVM "<Path to master image item with an additional disk >"
   -NetworkMapping <NetworkMapping > -ProvisioningSchemeName
   "<ProvisioningSchemeName >" -DataDisk "" -DataDiskPersistence
   "Persistent"  -Scope @() -VMCpuCount 4  -VMMemoryMB 6144  -TenancyType
   Shared  -FunctionalLevel "L7_20"
   ```

3. Adicione VMs ao catálogo usando o comando PowerShell `New-ProvVM`.

Atualização de imagem com disco de dados

Você pode atualizar a imagem usando `Publish-ProvMasterVMImage`, no entanto, você não pode atualizar uma imagem de um catálogo existente, contendo um disco de dados com uma imagem que não possui um disco de dados. Depois de atualizar a imagem:

- Para um catálogo persistente:
  - novas VMs no catálogo têm disco de SO e disco de dados atualizados. As VMs existentes não são atualizadas
- Para um catálogo não persistente:

- novas VMs no catálogo têm disco de SO e disco de dados atualizados. O disco de SO das VMs existentes é atualizado na próxima reinicialização, enquanto o disco de dados não é atualizado.

Excluir disco de dados

Se você excluir o catálogo, o disco de dados será excluído, a menos que você use a opção `forgetVM` ou `purgeDBOnly`. Se você excluir a VM, o disco de dados será excluído, a menos que você use a opção `forgetVM` ou `purgeDBOnly`.

Para catálogos de provisionamento sob demanda, nunca exclua o disco de dados.

Copiar tags em VMs

Você pode copiar tags em NICs e discos (disco de identidade, disco de cache de gravação e disco do SO) que são especificados no perfil da máquina para VMs recém-criadas em um catálogo de máquinas MCS. Você pode especificar essas tags em qualquer uma das fontes de perfil da máquina (instância de VM AWS ou versão de modelo de inicialização AWS). Este recurso é aplicável a catálogos de máquinas e VMs persistentes e não persistentes.

> **Nota:**

> - No console do AWS EC2, você não pode ver os valores de **Tag Network Interfaces** em **Launch Template Version Resource Tags**. No entanto, você pode executar o comando PowerShell `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` para ver as especificações da tag.
> - Se uma fonte de perfil de máquina (VM ou versão de modelo de inicialização) tiver duas interfaces de rede (eni-1 e eni-2), e eni-1 tiver a tag t1 e eni-2 tiver a tag t2, então a VM receberá as tags de ambas as interfaces de rede.

Filtrar instâncias de VM usando PowerShell

Uma instância de VM AWS que você usa como VM de perfil de máquina deve ser compatível para que o catálogo de máquinas seja criado e funcione corretamente. Para listar as instâncias de VM AWS que podem ser usadas como VMs de entrada de perfil de máquina, você pode usar o comando `Get-HypInventoryItem`. O comando pode paginar e filtrar o inventário de VMs disponíveis em uma unidade de hospedagem.

Paginação:

Get-HypInventoryItem suporta dois modos de paginação:

- O modo de paginação usa os parâmetros `-MaxRecords` e `-Skip` para retornar conjuntos de itens:
  - `-MaxRecords`: O padrão é **1**. Isso controla quantos itens retornar.
  - `-Skip`: O padrão é **0**. Isso controla quantos itens pular do início absoluto (ou fim absoluto) da lista no hypervisor.
- O modo de rolagem usa os parâmetros `-MaxRecords`, `-ForwardDirection` e `-ContinuationToken` para permitir a rolagem dos registros:
  - `-ForwardDirection`: O padrão é **True**. Isso é usado junto com `-MaxRecords` para retornar o próximo conjunto de registros correspondentes ou o conjunto anterior de registros correspondentes.
  - `-ContinuationToken`: Retorna os itens imediatamente depois (ou antes, se `ForwardDirection` for **false**), mas não incluindo o item fornecido em `ContinuationToken`.

Exemplos de paginação:

- Para retornar um único registro do modelo de máquina com o nome mais baixo. O campo `AdditionalData` tem o `TotalItemsCount` e o `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- Para retornar 10 registros do modelo de máquina com o nome mais baixo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- Para retornar um array de registros terminando com o nome mais alto:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- Para retornar um array de registros começando no modelo de máquina associado ao `ContinuationToken` fornecido:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

Filtragem:

Os seguintes parâmetros opcionais adicionais são suportados para filtragem. Você pode combinar esses parâmetros com as opções de paginação.

- `-ContainsName "my_name"`: Se a string fornecida corresponder a parte de um nome de AMI, a AMI será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: Se uma AMI tiver pelo menos uma dessas tags, ela será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **Nota:**
>
> Dois valores de tag são suportados. O valor de tag **Não Marcado** corresponde a itens que não possuem a tag fornecida em sua lista de tags. O valor de tag **Todos os valores** corresponde a itens que possuem a tag, independentemente do valor da tag. Caso contrário, a correspondência ocorre somente se o item tiver a tag e o valor for igual ao que é fornecido no filtro.

- `-Id "ami-0a2d913927e0352f3"`: Se a AMI corresponder ao ID fornecido, ela será incluída no resultado `Get`. Por exemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

Filtragem no parâmetro AdditionalData:

O parâmetro de filtro `AdditionalData` lista modelos ou VMs com base em sua capacidade, oferta de serviço ou qualquer propriedade que esteja em AdditionalData. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

Você também pode adicionar um `-Warn` parâmetro para indicar as VMs incompatíveis. As VMs são incluídas com um campo `AdditionalData` chamado **Warning**. Por exemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

Lista de SKUs de backup para VMs

As nuvens públicas podem, às vezes, ficar sem capacidade para um tipo específico de instância EC2 (“SKU primário”). Se a configuração da VM primária não estiver disponível, a VM não poderá iniciar, resultando em perda de tempo e interrupção dos negócios. Para resolver esses cenários, forneça uma lista de tipos de instância EC2 de backup (“SKUs de backup”) para os quais o MCS pode recorrer em caso de problemas relacionados à capacidade.

Use uma propriedade personalizada `BackupVmConfiguration` ao criar ou atualizar um catálogo de máquinas MCS para fornecer uma lista de tipos de instância EC2 de backup (“Lista de SKUs de Backup”).

Se a instância EC2 primária falhar, o MCS tenta recorrer aos tipos de instância EC2 de backup na ordem especificada. Se o MCS não conseguir recorrer a nenhum dos tipos de instância EC2 de backup fornecidos, uma mensagem de erro será exibida. Você pode então tentar ligar a instância EC2 primária novamente. Se isso falhar, o MCS tentará novamente os tipos de instância EC2 de backup.

A lista de SKUs de backup pode ter instâncias sob demanda.

Este recurso é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

Considerações importantes

- Você pode fornecer vários tipos de instância EC2 de backup na lista de SKUs de backup.
- A lista de SKUs de backup deve ser única.

- Uma instância EC2 de backup não pode ser a mesma que a instância EC2 primária.
- As instâncias EC2 de backup devem ser tipos de instância AWS válidos.
- Não especifique ofertas de serviço duplicadas. Exemplo: `BackupVmConfiguration,t2.small|t3.small|t2.small` não é válido.
- A oferta de serviço especificada na lista deve ser compatível com a configuração do catálogo de máquinas. Por exemplo, se o catálogo usar UEFI e a oferta de serviço especificada na lista de backup não o suportar, a criação ou atualização do catálogo falhará durante o pré-voo.
- Você pode modificar a lista de SKUs de backup de um catálogo existente usando o comando PowerShell `Set-ProvScheme`. Você pode modificar VMs existentes usando os comandos PowerShell `Set-ProvVM` e `Set-ProvVMUpdateTimeWindow`.

Configurar instâncias EC2 de backup

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um catálogo de Broker.
4. Crie um pool de identidades.
5. Adicione uma lista de instâncias EC2 de backup usando a propriedade personalizada `BackupVmConfiguration` e crie um esquema de provisionamento. Por exemplo:

```
$serviceOffering = "XDHyp:\HostingUnits\$hostingUnitName\T3 Medium
Instance.serviceoffering"

$customProperties =
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small|t3.large;"

$createdProvScheme = New-ProvScheme -ProvisioningSchemeName
$provisioningSchemeName -HostingUnitName $hostingUnitName
-IdentityPoolName $provisioningSchemeName -NetworkMapping
$networkMapping -SecurityGroup $securityGroupPath -ServiceOffering
$serviceOffering -MasterImageVM $masterImageVm -CustomProperties
$customProperties
```

6. Atualize o BrokerCatalog com o Id exclusivo do esquema de provisionamento.
7. Crie e adicione VMs ao catálogo.

Você também pode adicionar instâncias EC2 de backup usando o Studio:

Na página **Máquinas Virtuais**, clique em **Tamanho secundário** (opcional). Na janela **Tamanho da máquina secundária**, as VMs listadas têm tipos de VM Spot e Regular. Você pode selecionar até 10 tamanhos de máquina secundários. Uma vez que as 10 VMs são selecionadas, as outras VMs listadas são desabilitadas para seleção posterior. Clique em **Avançar**. No painel **Tamanho da máquina secundária**, você pode selecionar vários tamanhos de máquina e arrastar e soltar para alterar a ordem de prioridade. Clique em **Concluído**. Os tamanhos de máquina selecionados aparecem em Tamanho secundário (opcional). Clique no ícone de edição para editar conforme necessário. Consulte Criar um catálogo usando o Studio.

Criar um catálogo usando instância Spot do AWS

Em comparação com as instâncias sob demanda, as instâncias Spot oferecem economia de custos de até 90%. As instâncias Spot podem ser interrompidas pelo Amazon EC2 se a capacidade se tornar indisponível, tornando-as adequadas apenas para aplicativos e desktops não críticos.

Para obter informações sobre instâncias Spot, consulte o documento do AWS Spot Instances.

Além disso, você pode usar instâncias Spot como tipo de instância EC2 primária e instância EC2 de backup. Você pode fornecer uma lista de tipos de instância EC2 de backup (“SKUs de Backup” que podem ser instâncias sob demanda e Spot) usando o PowerShell, para os quais o MCS pode recorrer em caso de problemas relacionados à capacidade.

Considerações importantes**

- Você deve criar um catálogo de instâncias Spot apenas com o fluxo de trabalho de perfil de máquina.
- Apenas um tipo de solicitação de instância Spot persistente é suportado. Uma solicitação de instância Spot única não é suportada.
- Apenas os comportamentos de interrupção **Parar** e **Hibernar** são suportados.
- Você pode alterar a configuração de um catálogo existente de instâncias sob demanda para instâncias Spot e vice-versa. No entanto, alterar uma instância EC2 de sob demanda para Spot é complexo. Consulte a documentação da AWS Alternar uma instância EC2 de sob demanda para preço Spot.
- Ao excluir uma instância Spot provisionada, cancele a solicitação de instância Spot existente. Caso contrário, a AWS criará uma nova instância Spot.

Etapas para criar um catálogo usando instâncias Spot da AWS

1. Crie uma fonte de perfil de máquina com instância Spot. Para as etapas de criação de uma instância Spot, consulte Criar uma solicitação de instância Spot.
2. Crie um catálogo de máquinas usando um perfil de máquina com o comando PowerShell `New-ProvScheme`. Você pode atualizar um catálogo usando o comando `Set-ProvScheme`.

Usar instâncias Spot como SKU de backup

Você pode usar instâncias Spot como tipo de instância EC2 primária e instância EC2 de backup. Você pode fornecer uma lista de tipos de instância EC2 de backup (“SKUs de Backup” que podem ser instâncias sob demanda e Spot) usando PowerShell para que o MCS possa recorrer em problemas relacionados à capacidade.

> **Nota:**
>
> Você pode especificar instâncias Spot duplicadas na lista de SKUs de backup. Exemplo: `BackupVmConfiguration,t2.small:Spot|t2.small|t3.small` é válido.

Permissões necessárias

Você precisa das seguintes permissões se usar a instância Spot como uma instância EC2 primária ou de backup:

- `ec2:DescribeSpotInstanceRequests`
- `ec2:CancelSpotInstanceRequests`

Configurar instâncias Spot de backup

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos do Citrix.
3. Crie um catálogo do Broker.
4. Crie um pool de identidades.
5. Adicione uma lista de instâncias EC2 de backup usando a propriedade personalizada `BackupVmConfiguration` e crie um esquema de provisionamento. Por exemplo:

```
$serviceOffering \= "XDHyp:\\HostingUnits\\$hostingUnitName\\T3 Medium
Instance.serviceoffering"
```

```
$customProperties \=
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small:Spot|t3.large:Spot"


$createdProvScheme \= New-ProvScheme \-ProvisioningSchemeName
$provisioningSchemeName \-HostingUnitName $hostingUnitName \-
IdentityPoolName $provisioningSchemeName \-NetworkMapping
$networkMapping \-SecurityGroup $securityGroupPath \-ServiceOffering
$serviceOffering \-MasterImageVM $masterImageVm \-CustomProperties
$customProperties
```

6. Atualize o BrokerCatalog com o ID exclusivo do esquema de provisionamento.
7. Crie e adicione VMs ao catálogo.

Onde ir a seguir

- Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.
- Para revisar todo o processo de configuração, consulte Planejar e construir uma implantação.
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo AWS EC2.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com AWS EC2
- Criar catálogos de máquinas

Criar um catálogo do Google Cloud Platform

(/pt-br/citrix-daas/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de nuvem do Google.

> **Nota:**

> Antes de criar um catálogo do Google Cloud Platform (GCP), você precisa concluir a criação de uma conexão com o GCP. Consulte (/pt-br/citrix-daas/install-configure/connections/connection-gcp.html).

Preparar uma instância de VM mestre e um disco persistente

> **Dica:**

> Disco persistente é o termo do Google Cloud para disco virtual.

> Para preparar sua instância de VM mestre, crie e configure uma instância de VM com propriedades que correspondam à configuração desejada para as instâncias VDA clonadas em seu catálogo de máquinas planejado. A configuração não se aplica apenas ao tamanho e tipo da instância. Ela também inclui atributos da instância, como metadados, tags, atribuições de GPU, tags de rede e propriedades da conta de serviço.

Como parte do processo de masterização, o MCS usa sua instância de VM mestre para criar o *modelo de instância* do Google Cloud. O modelo de instância é então usado para criar as instâncias VDA clonadas que compõem o catálogo de máquinas. As instâncias clonadas herdam as propriedades (exceto as propriedades de VPC, sub-rede e disco persistente) da instância de VM mestre a partir da qual o modelo de instância foi criado.

Depois de configurar as propriedades da instância de VM mestre de acordo com suas especificações, inicie a instância e, em seguida, prepare o disco persistente para a instância.

Recomendamos que você crie manualmente um snapshot do disco ou uma imagem do disco. Isso permite que você use uma convenção de nomenclatura significativa para rastrear versões, oferece mais opções para gerenciar versões anteriores de sua imagem mestre e economiza tempo na criação do catálogo de máquinas. Se você não criar seu próprio snapshot, o MCS criará um snapshot temporário para você (que é excluído no final do processo de provisionamento). A criação manual de um snapshot multirregional do disco ou imagem do SO também permite que você use a mesma imagem mestre para catálogos de máquinas em diferentes regiões do GCP.

Habilitar seleção de zona

O Citrix DaaS™ oferece suporte à seleção de zona. Com a seleção de zona, você especifica as zonas onde deseja criar VMs. Com a seleção de zona, os administradores podem colocar nós de

locatário único em zonas de sua escolha. Para configurar a locação única, você deve concluir o seguinte no Google Cloud:

- Reservar um nó de locatário único do Google Cloud
- Criar a imagem mestre do VDA

Reservar um nó de locatário único do Google Cloud

Para reservar um nó de locatário único, consulte a documentação do Google Cloud.

> **Importante:**
>
> Um modelo de nó é usado para indicar as características de desempenho do sistema que é reservado no grupo de nós. Essas características incluem o número de vGPUs, a quantidade de memória alocada ao nó e o tipo de máquina usado para máquinas criadas no nó. Para obter mais informações, consulte a documentação do Google Cloud.

Criar a imagem mestre do VDA

Para implantar máquinas no nó de locatário único com sucesso, você precisa seguir etapas extras ao criar uma imagem mestre de VM. As instâncias de máquina no Google Cloud têm uma propriedade chamada *rótulos de afinidade de nó*. As instâncias usadas como imagens mestras para catálogos implantados no nó de locatário único exigem um *rótulo de afinidade de nó* que corresponda ao nome do **grupo de nós de destino**. Para conseguir isso, tenha em mente o seguinte:

- Para uma nova instância, defina o rótulo no console do Google Cloud ao criar uma instância. Para obter detalhes, consulte Provisionar uma VM de locatário único.
- Para uma instância existente, defina o rótulo usando a linha de comando **gcloud**. Para obter detalhes, consulte Configurar rótulos de afinidade de nó.

> **Nota:**
>
> Se você pretende usar a locação única com uma VPC compartilhada, consulte Virtual Private Cloud Compartilhada.

Criar um catálogo de máquinas

> **Nota:**
>
> Crie seus recursos antes de criar um catálogo de máquinas. Use as convenções de nomenclatura estabelecidas pelo Google Cloud ao configurar catálogos de máquinas. Consulte Diretrizes de nomenclatura de buckets e objetos para obter mais informações.

> Você pode criar um catálogo de máquinas de duas maneiras:

- Studio
- PowerShell. Consulte Gerenciar Citrix DaaS usando SDKs remotos do PowerShell. Para obter informações sobre como implementar recursos específicos usando o PowerShell, consulte Usar PowerShell

Criar um catálogo de máquinas usando o Studio

Siga as orientações em Criar catálogos de máquinas. A descrição a seguir é exclusiva para catálogos do Google Cloud.

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione **Criar Catálogo de Máquinas** na barra de ações.
3. Na página **Tipo de Máquina**, selecione **SO de várias sessões** e, em seguida, selecione **Avançar**. O Citrix DaaS também oferece suporte a SO de sessão única.
4. Na página **Gerenciamento de Máquinas**, selecione as opções **Máquinas que têm o gerenciamento de energia ativado** e **Citrix Machine Creation Services™** e, em seguida, selecione **Avançar**. Se houver vários recursos, selecione um no menu.
5. Na página **Imagem**, conclua estas etapas conforme necessário e, em seguida, clique em **Avançar**.

    a. Selecione a imagem mestre. Você pode selecionar os seguintes tipos de imagem:

    - Máquina Virtual (cujas regiões são as mesmas das unidades de hospedagem selecionadas).
    - Instantâneos (suportam instantâneos multirregionais).
    - Imagem do SO (suporta imagens públicas e não públicas multirregionais). Se você quiser usar a funcionalidade de locação única, certifique-se de selecionar uma imagem cuja propriedade de grupo de nós esteja configurada corretamente. Consulte Habilitar seleção de zona.

b. Na página **Selecionar um perfil de máquina**, selecione recursos na guia **Máquina virtual** ou na guia **Modelos de instância**.

> **Nota:**
>
> - Atualmente, as VMs neste catálogo herdam as configurações de armazenamento, tipo de máquina e criptografia de disco do perfil de máquina selecionado.
> - Se você selecionar um modelo de instância como perfil da máquina, todas as zonas serão selecionadas por padrão. Você pode selecionar as zonas conforme necessário.

c. Selecione o nível funcional mínimo para o catálogo.

6. Na página **Armazenamento**, selecione o tipo de armazenamento usado para conter o sistema operacional para este catálogo de máquinas. Cada uma das seguintes opções de armazenamento tem características únicas de preço e desempenho. Um disco de identidade é sempre criado usando o disco persistente padrão zonal.

   - Disco persistente padrão
   - Disco persistente balanceado
   - Disco persistente SSD

   Para obter detalhes sobre as opções de armazenamento do Google Cloud, consulte Opções de armazenamento.

7. Na página **Máquinas Virtuais**, especifique quantas VMs você deseja criar, visualize a especificação detalhada das VMs, selecione o tipo de máquina do Google Cloud e, em seguida, selecione **Avançar**. Se você usar grupos de nós de locatário único para catálogos de máquinas, certifique-se de selecionar **apenas** as zonas onde os nós de locatário único reservados estão disponíveis. Consulte Habilitar seleção de zona.

   > **Nota**:
   >
   > O **tipo de máquina do Google Cloud** é selecionado automaticamente com base no perfil da máquina escolhido. Você pode selecionar um tipo de máquina diferente, se necessário.

8. Na página **Configurações de Disco**, você pode configurar as seguintes opções:

   - Escolha se deseja habilitar o cache de write-back. Depois de habilitar o cache de write-back, você pode fazer o seguinte:

     - Configure o tamanho do disco e da RAM usados para armazenar dados temporários em cache. Para obter mais informações, consulte Configurar cache para dados temporários.
     - Selecione o tipo de armazenamento para o disco de cache de write-back. As seguintes opções de armazenamento estão disponíveis para uso no disco de cache de write-back:

       - Disco persistente padrão
       - Disco persistente balanceado
       - Disco persistente SSD

       Para obter detalhes sobre as opções de armazenamento do Google Cloud, consulte Opções de armazenamento.
     - Selecione o tipo para o disco de cache de write-back.

       - **Usar disco de cache de write-back não persistente**. Se selecionado, o disco de cache de write-back não persiste para as VMs provisionadas. O disco é excluído durante os ciclos de energia e quaisquer dados redirecionados para o disco serão perdidos.
       - **Usar disco de cache de write-back persistente**. Se selecionado, o disco de cache de write-back persiste para as VMs provisionadas. Habilitar esta opção aumenta seus custos de armazenamento.

   - Quando a otimização de armazenamento MCS (MCS I/O) está habilitada, você pode fazer o seguinte:

     - Escolha se deseja reter discos de sistema para VDAs durante os ciclos de energia. Para obter mais informações, consulte Habilitando atualizações de otimização de armazenamento MCS.
     - Atualize os tamanhos de memória e cache de disco.

   - Escolha se deseja usar sua própria chave para proteger o conteúdo do disco. Para usar o recurso, você deve primeiro criar suas próprias Chaves de Criptografia Gerenciadas pelo

Cliente (CMEKs). Para obter mais informações, consulte Usar Chaves de Criptografia Gerenciadas pelo Cliente (CMEK).

> **Nota:**
>
> Está disponível apenas na interface do Studio.
>
> Depois de criar as chaves, você pode selecionar uma dessas chaves na lista. Você não pode alterar a chave depois de criar o catálogo. O Google Cloud não oferece suporte à rotação de chaves em discos persistentes ou imagens existentes. Portanto, depois de provisionar um catálogo, o catálogo é vinculado a uma versão específica da chave. Se essa chave for desabilitada ou destruída, as instâncias e os discos criptografados com ela se tornarão inutilizáveis até que a chave seja reativada ou restaurada.

As configurações da Chave de Criptografia Gerenciada pelo Cliente (CMEK) seguem uma sequência de prioridade conforme abaixo:

- A CMEK personalizada de um catálogo tem a mais alta prioridade.
- Se o perfil de máquina selecionado estiver criptografado, as configurações de CMEK usarão automaticamente o CMEK do perfil de máquina como a próxima prioridade.
- Se o perfil de máquina selecionado não estiver criptografado, as configurações de CMEK usarão automaticamente o CMEK da imagem mestre.

9. Na página **Identidades da Máquina**, selecione uma conta do Active Directory e, em seguida, selecione **Avançar**.

   - Se você selecionar **Criar novas contas do Active Directory**, selecione um domínio e, em seguida, insira a sequência de caracteres que representa o esquema de nomenclatura para as contas de computador de VM provisionadas criadas no Active Directory. O esquema de nomenclatura da conta pode conter de 1 a 64 caracteres e não pode conter espaços em branco, caracteres não ASCII ou caracteres especiais.
   - Se você selecionar **Usar contas existentes do Active Directory**, selecione **Procurar** para navegar até as contas de computador do Active Directory existentes para as máquinas selecionadas.

10. Na página **Credenciais de Domínio**, selecione **Inserir credenciais**, digite o nome de usuário e a senha, selecione **Salvar** e, em seguida, selecione **Avançar**.

- A credencial que você digita deve ter permissões para realizar operações de conta do Active Directory.

11. Na página **Escopos**, selecione os escopos para o catálogo de máquinas e, em seguida, selecione **Avançar**.

    - Você pode selecionar escopos opcionais ou selecionar **escopo personalizado** para personalizar os escopos conforme necessário.

12. Na página **Resumo**, confirme as informações, especifique um nome para o catálogo e, em seguida, selecione **Concluir**.

> **Nota:**
>
> O nome do catálogo pode conter de 1 a 39 caracteres e não pode conter apenas espaços em branco ou os caracteres `\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`.

A criação do catálogo de máquinas pode levar muito tempo para ser concluída. Quando concluído, o catálogo é listado. Você pode verificar se as máquinas são criadas nos grupos de nós de destino no console do Google Cloud.

Importar máquinas do Google Cloud criadas manualmente

Usando este recurso, você pode:

- Importar máquinas OS de multi-sessão do Google Cloud criadas manualmente para um catálogo Citrix DaaS.
- Remover máquinas OS de multi-sessão do Google Cloud criadas manualmente de um catálogo Citrix DaaS.
- Usar os recursos existentes de gerenciamento de energia do Citrix DaaS para gerenciar a energia de máquinas OS de multi-sessão do Google Cloud Windows. Por exemplo, definir um agendamento de reinício para essas máquinas.

Essa funcionalidade não exige alterações em um fluxo de trabalho de provisionamento existente do Citrix DaaS, nem a remoção de qualquer recurso existente.

Recomenda-se usar o MCS para provisionar máquinas no Studio em vez de importar máquinas do Google Cloud criadas manualmente.

Nuvem Privada Virtual Compartilhada

Nuvens Privadas Virtuais Compartilhadas (VPCs) compreendem um projeto host, a partir do qual as sub-redes compartilhadas são disponibilizadas, e um ou mais projetos de serviço que usam o recurso. As VPCs Compartilhadas são opções desejáveis para instalações maiores porque fornecem controle centralizado, uso e administração de recursos corporativos compartilhados da nuvem do Google. Para mais informações, consulte o site de Documentação do Google.

Com este recurso, o Machine Creation Services (MCS) oferece suporte ao provisionamento e gerenciamento de catálogos de máquinas implantados em VPCs Compartilhadas. Este suporte, que é funcionalmente equivalente ao suporte atualmente fornecido em VPCs locais, difere em duas áreas:

- Você deve conceder permissões extras à Conta de Serviço usada para criar a conexão do host. Este processo permite que o MCS acesse e use os Recursos da VPC Compartilhada. Consulte Novas permissões necessárias.
- Você deve criar duas regras de firewall, uma para entrada e outra para saída. Essas regras de firewall são usadas durante o processo de masterização da imagem. Consulte Regras de Firewall.

Para obter informações sobre como configurar a VPC compartilhada, consulte Configurar a VPC compartilhada.

Novas permissões necessárias

Uma conta de serviço do Google Cloud com permissões específicas é necessária ao criar a conexão do host. Essas permissões adicionais devem ser concedidas a quaisquer contas de serviço usadas para criar conexões de host baseadas em VPC Compartilhada.

> **Dica:**
>
> Essas permissões adicionais não são novas para o Citrix DaaS. Elas são usadas para facilitar a implementação de VPCs locais. Com as VPCs Compartilhadas, essas permissões adicionais permitem o acesso a outros recursos de VPC compartilhada.

Um máximo de quatro permissões extras devem ser concedidas à conta de serviço associada à conexão do host para suportar o VPC Compartilhado:

- **compute.firewalls.list** - Esta permissão é obrigatória. Ela permite que o MCS recupere a lista de regras de firewall presentes no VPC Compartilhado.

- **compute.networks.list** - Esta permissão é obrigatória. Ela permite que o MCS identifique as redes VPC Compartilhadas disponíveis para a conta de serviço.
- **compute.subnetworks.list** – Esta permissão é opcional, dependendo de como você usa os VPCs. Ela permite que o MCS identifique as sub-redes dentro dos VPCs Compartilhados visíveis. Esta permissão já é exigida ao usar VPCs locais, mas também deve ser atribuída no projeto host do VPC Compartilhado.
- **compute.subnetworks.use** - Esta permissão é opcional, dependendo de como você usa os VPCs. É necessário usar recursos de sub-rede nos catálogos de máquinas provisionados. Esta permissão já é exigida para usar VPCs locais, mas também deve ser atribuída no projeto host do VPC Compartilhado.

Ao usar essas permissões, considere que existem diferentes abordagens com base no tipo de permissão usada para criar o catálogo de máquinas:

- Permissão em nível de projeto:
  - Permite acesso a todos os VPCs Compartilhados dentro do projeto host.
  - Exige que as permissões `compute.subnetworks.list` e `compute.subnetworks.use` sejam atribuídas à conta de serviço.
- Permissão em nível de sub-rede:
  - Permite acesso a sub-redes específicas dentro do VPC Compartilhado.
  - As permissões `compute.subnetworks.list` e `compute.subnetworks.use` são intrínsecas à atribuição em nível de sub-rede e, portanto, não precisam ser atribuídas diretamente à conta de serviço.

Selecione a abordagem que melhor se adapta às suas necessidades organizacionais e padrões de segurança.

> **Dica:**
>
> Para obter mais informações sobre as diferenças entre permissões em nível de projeto e em nível de sub-rede, consulte Administradores de Projeto de Serviço.

Regras de Firewall

Durante a preparação de um catálogo de máquinas, uma imagem de máquina é preparada para servir como o disco do sistema da imagem mestre para o catálogo. Quando esse processo ocorre, o disco é temporariamente anexado a uma máquina virtual. Essa VM deve ser executada em um ambiente isolado que impede todo o tráfego de rede de entrada e saída. Isso é realizado por meio de um par de regras de firewall de negação total; uma para tráfego de entrada e outra para tráfego de saída. Ao usar VPCs locais do Google Cloud, o MCS cria esse firewall na rede local e o aplica à máquina para masterização. Após a conclusão da masterização, a regra de firewall é removida da imagem.

Recomendamos manter o número de novas permissões necessárias para usar VPCs Compartilhadas no mínimo. As VPCs Compartilhadas são recursos corporativos de nível superior e geralmente possuem protocolos de segurança mais rígidos em vigor. Por esse motivo, crie um par de regras de firewall no projeto host nos recursos da VPC compartilhada, uma para entrada e outra para saída. Atribua a mais alta prioridade a elas. Aplique uma nova tag de destino a cada uma dessas regras, usando o seguinte valor:

```
citrix-provisioning-quarantine-firewall
```

Quando o MCS cria ou atualiza um catálogo de máquinas, ele procura por regras de firewall que contenham esta tag de destino. Em seguida, ele examina as regras quanto à correção e as aplica à máquina usada para preparar a imagem mestre para o catálogo. Se as regras de firewall não forem encontradas, ou se as regras forem encontradas, mas as regras ou suas prioridades estiverem incorretas, uma mensagem semelhante à seguinte aparecerá:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag ‘citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."
```

Configurar a VPC compartilhada

Antes de adicionar a VPC Compartilhada como uma conexão de host no Studio do Citrix DaaS, conclua as seguintes etapas para adicionar contas de serviço do projeto no qual você pretende provisionar:

1. Criar uma função IAM.
2. Adicionar uma conta de serviço à função IAM do projeto host.
3. Adicionar a conta de serviço de compilação em nuvem à VPC compartilhada.
4. Criar regras de firewall.

CRIAR UMA FUNÇÃO IAM

Determine o nível de acesso da função:

- *Acesso em nível de projeto*, ou
- Um modelo mais restrito usando *acesso em nível de sub-rede*.

Acesso em nível de projeto para função IAM. Para a função IAM em nível de projeto, inclua as seguintes permissões:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Para criar uma função IAM em nível de projeto:

1. No console do Google Cloud, navegar até **IAM e administrador > Funções**.
2. Na página **Funções**, selecione **CRIAR FUNÇÃO**.
3. Na página **Criar função**, especifique o nome da função. Selecione **ADICIONAR PERMISSÕES**.
    a. Na página **Adicionar permissões**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filtrar tabela**. Selecione a permissão e, em seguida, selecione **ADICIONAR**.
    b. Selecione **CRIAR**.

Função IAM em nível de sub-rede. Esta função omite a adição das permissões `compute.subnetworks.list` e `compute.subnetworks.use` após selecionar **CRIAR FUNÇÃO**. Para este nível de acesso IAM, as permissões `compute.firewalls.list` e `compute.networks.list` devem ser aplicadas à nova função.

Para criar uma função IAM em nível de sub-rede:

1. No console do Google Cloud, navegar até **Rede VPC** > **VPC compartilhada**. A página **VPC compartilhada** é exibida, mostrando as sub-redes das redes VPC compartilhadas que o projeto host contém.
2. Na página **VPC Compartilhada**, selecione a sub-rede que você deseja acessar.
3. No canto superior direito, selecione **ADICIONAR MEMBRO** para adicionar uma conta de serviço.

4. Na página **Adicionar membros**, conclua estas etapas:
    a. No campo **Novos membros**, digite o nome da sua conta de serviço e, em seguida, selecione sua conta de serviço no menu.
    b. Selecione o campo **Selecionar um papel** e, em seguida, **Usuário da Rede de Computação**.
    c. Selecione **SALVAR**.
5. No console do Google Cloud, navegar para **IAM e Administrador** > **Funções**.
6. Na página **Funções**, selecione **CRIAR FUNÇÃO**.
7. Na página **Criar Função**, especifique o nome da função. Selecione **ADICIONAR PERMISSÕES**.
    a. Na página **Adicionar permissões**, adicione permissões à função, individualmente. Para adicionar uma permissão, digite o nome da permissão no campo **Filtrar tabela**. Selecione a permissão e, em seguida, selecione **ADICIONAR**.
    b. Selecione **CRIAR**.

ADICIONAR UMA CONTA DE SERVIÇO À FUNÇÃO IAM DO PROJETO HOST

Após criar uma função IAM, siga as etapas abaixo para adicionar uma conta de serviço para o projeto host:

1. No console do Google Cloud, navegar para o projeto host e, em seguida, para **IAM e Administrador > IAM**.
2. Na página **IAM**, selecione **ADICIONAR** para adicionar uma conta de serviço.
3. Na página **Adicionar membros**:
    a. No campo **Novos membros**, digite o nome da sua conta de serviço e selecione sua conta de serviço no menu.
    b. Selecione um campo de função, digite a função IAM que você criou e selecione a função no menu.
    c. Selecione **SALVAR**.

A conta de serviço agora está configurada para o projeto host.

ADICIONAR A CONTA DE SERVIÇO DE COMPILAÇÃO EM NUVEM AO VPC COMPARTILHADO

Cada assinatura do Google Cloud tem uma conta de serviço que é nomeada após o número de ID do projeto, seguido por `cloudbuild.gserviceaccount`. Por exemplo: `705794712345@cloudbuild.gserviceaccount`.

Você pode determinar o número de ID do projeto para o seu projeto navegando até **Visão geral da nuvem > Painel** no console do Google Cloud. O ID do projeto e o número do projeto são exibidos no cartão de informações do projeto do Painel do projeto:

Execute as seguintes etapas para adicionar a conta de serviço do Cloud Build ao VPC Compartilhado:

1. No console do Google Cloud, navegar até o projeto host e depois para **IAM e administrador** > **IAM**.
2. Na página **Permissões**, selecione **ADICIONAR** para adicionar uma conta.
3. Na página **Adicionar membros**, conclua estas etapas:
    a. No campo **Novos membros**, digite o nome da conta de serviço do Cloud Build e selecione sua conta de serviço no menu.
    b. Selecione o campo **Selecionar uma função**, digite `Computer Network User` e selecione a função no menu.
    c. Selecione **SALVAR**.

CRIAR REGRAS DE FIREWALL

Como parte do processo de masterização, o MCS copia a imagem de máquina selecionada e a usa para preparar o disco do sistema da imagem mestre para o catálogo. Durante a masterização, o MCS anexa o disco a uma máquina virtual temporária, que então executa scripts de preparação. Esta VM deve ser executada em um ambiente isolado que proíba todo o tráfego de rede de entrada e saída.

Para criar um ambiente isolado, o MCS requer duas regras de firewall *negar tudo* (uma regra de entrada e uma regra de saída). Portanto, crie duas regras de firewall (Entrada e Saída) no *Projeto Host* da seguinte forma:

1. No console do Google Cloud, navegar até o projeto host e depois para **Rede VPC > Firewall**.
2. Na página **Firewall**, selecione **CRIAR REGRA DE FIREWALL**.
3. Na página **Criar uma regra de firewall**, preencha o seguinte:
    - **Nome**. Digite um nome para a regra.

- **Rede**. Selecione a rede VPC Compartilhada à qual a regra de firewall de entrada se aplica.
- **Prioridade**. Quanto menor o valor, maior a prioridade da regra. Recomendamos um valor pequeno (por exemplo, 10).
- **Direção do tráfego**. Selecione **Entrada**.
- **Ação na correspondência**. Selecione **Negar**.
- **Destinos**. Use o padrão, **Tags de destino especificadas**.
- **Tags de destino**. Digite `citrix-provisioning-quarantine-firewall`.
- **Filtro de origem**. Use o padrão, **Intervalos de IP**.
- **Intervalos de IP de origem**. Digite um intervalo que corresponda a todo o tráfego. Digite `0.0.0.0/0`.
- **Protocolos e portas**. Selecione **Negar tudo**.

4. Selecione **CRIAR** para criar a regra.
5. Repita as etapas para criar outra regra. Para **Direção do tráfego**, selecione **Saída**.

Usar chaves de criptografia gerenciadas pelo cliente (CMEK)

> **Observação:**

> O suporte para CMEK no GCP está atualmente em Pré-visualização.

> Você pode usar chaves de criptografia gerenciadas pelo cliente (CMEK) para catálogos MCS. Ao usar essa funcionalidade, você atribui a função `CryptoKey Encrypter/Decrypter` do Google Cloud Key Management Service ao Agente de Serviço do Compute Engine. A conta do Citrix DaaS deve ter as permissões corretas no projeto onde a chave está armazenada. Consulte Atribuir permissões à conta do Citrix DaaS. Consulte Ajudando a proteger recursos usando chaves do Cloud KMS para obter mais informações.

Seu Agente de Serviço do Compute Engine está no seguinte formato: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`. Este formato é diferente da Conta de Serviço padrão do Compute Engine.

> **Observação:**

> Esta Conta de Serviço do Compute Engine pode não aparecer na exibição **Permissões de IAM** do Google Console. Nesses casos, use o comando `gcloud` conforme descrito em Ajudando a proteger recursos usando chaves do Cloud KMS.

Atribuir permissões à conta do Citrix DaaS

As permissões do Google Cloud KMS podem ser configuradas de várias maneiras. Você pode fornecer permissões KMS *no nível do projeto* ou permissões KMS *no nível do recurso*. Consulte Permissões e funções para obter mais informações.

PERMISSÕES KMS NO NÍVEL DO PROJETO

Uma opção é fornecer à conta do Citrix DaaS permissões no nível do projeto para navegar pelos recursos do Cloud KMS. Para fazer isso, crie uma função personalizada e adicione as seguintes permissões:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Atribua esta função personalizada à sua conta Citrix DaaS. Isso permite que você navegue pelas chaves regionais no projeto relevante no inventário.

PERMISSÕES KMS EM NÍVEL DE RECURSO

Para a outra opção, permissões em nível de recurso, no console do Google Cloud, navegue até o `cryptoKey` que você usa para provisionamento MCS. Adicione a conta Citrix DaaS a um conjunto de chaves ou a uma chave que você usa para provisionamento de catálogo.

> **Dica:**

> Com esta opção, você não pode navegar pelas chaves regionais do seu projeto no inventário porque a conta Citrix DaaS não tem permissões de listagem em nível de projeto nos recursos do Cloud KMS. No entanto, você ainda pode provisionar um catálogo usando CMEK especificando o `cryptoKeyId` correto nas propriedades personalizadas `ProvScheme`. Consulte Criar um catálogo com CMEK usando propriedades personalizadas.

Rotação de chaves gerenciadas pelo cliente

O Google Cloud não oferece suporte à rotação de chaves em discos persistentes ou imagens existentes. Uma vez que uma máquina é provisionada, ela está vinculada à versão da chave em uso no momento em que foi criada. No entanto, uma nova versão da chave pode ser criada e essa nova chave é usada para máquinas recém-provisionadas ou recursos criados quando um catálogo é atualizado com uma nova imagem mestre.

CONSIDERAÇÕES IMPORTANTES SOBRE CONJUNTOS DE CHAVES

Os conjuntos de chaves não podem ser renomeados ou excluídos. Além disso, você pode incorrer em cobranças imprevistas ao configurá-los. Ao excluir ou remover um conjunto de chaves, o Google Cloud exibe uma mensagem de erro:

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

Dica:

Para obter mais informações, consulte Editar ou excluir um conjunto de chaves do console.

Compatibilidade de acesso uniforme em nível de bucket

O Citrix DaaS é compatível com a política de controle de acesso uniforme no nível do bucket no Google Cloud. Essa funcionalidade aumenta o uso da política de IAM que concede permissões a uma conta de serviço para permitir a manipulação de recursos, incluindo buckets de armazenamento. Com o controle de acesso uniforme no nível do bucket, o Citrix DaaS permite que você use uma lista de controle de acesso (ACL) para controlar o acesso a buckets de armazenamento ou objetos armazenados neles. Consulte Acesso uniforme no nível do bucket

para obter informações gerais sobre o acesso uniforme no nível do bucket do Google Cloud. Para obter informações de configuração, consulte Exigir acesso uniforme no nível do bucket.

Usar PowerShell

Esta seção detalha como realizar as seguintes tarefas usando o PowerShell:

- Criar um catálogo com disco de cache de write-back persistente
- Melhorar o desempenho de inicialização com MCSIO
- Criar um catálogo com CMEK usando propriedades personalizadas
- Criar um catálogo de máquinas usando um perfil de máquina
- Criar um catálogo de máquinas com perfil de máquina como um modelo de instância
- Criar um catálogo com VM blindada
- Criar VMs do Windows 11 no nó de locatário único
- VMs e discos com rótulos herdados

Criar um catálogo com disco de cache de write-back persistente

Para configurar um catálogo com disco de cache de write-back persistente, use o comando PowerShell `New-ProvScheme CustomProperties`.

> **Dica:**
>
> Use o parâmetro PowerShell `New-ProvScheme CustomProperties` apenas para conexões de hospedagem baseadas em nuvem. Se você quiser provisionar máquinas usando um disco de cache de write-back persistente para uma solução local (por exemplo, XenServer®), o PowerShell não é necessário porque o disco persiste automaticamente.
>
> Este comando suporta uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de write-back persiste para máquinas provisionadas por MCS. A propriedade `PersistWBC` é usada apenas quando o parâmetro `UseWriteBackCache` é especificado e quando o parâmetro `WriteBackCacheDiskSize` é definido para indicar que um disco é criado.

> **Nota:**

> Esse comportamento se aplica tanto ao Azure quanto ao GCP, onde o disco de cache de write-back MCSIO padrão é excluído e recriado durante o ciclo de energia. Você pode optar por manter o disco para evitar a exclusão e recriação do disco de cache de write-back MCSIO.

> Exemplos de propriedades encontradas no parâmetro `CustomProperties` antes de suportar `PersistWBC` incluem:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

> **Nota:**
>
> Este exemplo se aplica apenas ao Azure. As propriedades são diferentes no ambiente GCP.

> Ao usar essas propriedades, considere que elas contêm valores padrão se as propriedades forem omitidas do parâmetro `CustomProperties`. A propriedade `PersistWBC` tem dois valores possíveis: **true** ou **false**.

Definir a propriedade `PersistWBC` como **true** não exclui o disco de cache de write-back quando o administrador do Citrix DaaS desliga a máquina da interface de gerenciamento.

Definir a propriedade `PersistWBC` como **false** exclui o disco de cache de write-back quando o administrador do Citrix DaaS desliga a máquina da interface de gerenciamento.

> **Nota:**

Se a propriedade `PersistWBC` for omitida, a propriedade assume o valor padrão **false** e o cache de write-back é excluído quando a máquina é desligada da interface de gerenciamento.

Por exemplo, usando o parâmetro `CustomProperties` para definir `PersistWBC` como true:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

Importante:

A propriedade `PersistWBC` só pode ser definida usando o cmdlet PowerShell `New-ProvScheme`. Tentar alterar o `CustomProperties` de um esquema de provisionamento após a criação não tem impacto no catálogo de máquinas e na persistência do disco de cache de write-back quando uma máquina é desligada.

Por exemplo, defina `New-ProvScheme` para usar o cache de write-back enquanto define a propriedade `PersistWBC` como true:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
```

```
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Melhorar o desempenho de inicialização com MCSIO

Você pode melhorar o desempenho de inicialização para discos gerenciados do Azure e GCP quando o MCSIO está habilitado. Use a propriedade personalizada do PowerShell `PersistOSDisk` no comando `New-ProvScheme` para configurar esse recurso. As opções associadas a `New-ProvScheme` incluem:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource``````````````Groups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

Para habilitar esse recurso, defina a propriedade personalizada `PersistOSDisk` como **true**. Por exemplo:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
```

```
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Criar um catálogo com CMEK usando propriedades personalizadas

Ao criar seu Esquema de Provisionamento via PowerShell, especifique uma propriedade `CryptoKeyId` em `ProvScheme CustomProperties`. Por exemplo:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

O `cryptoKeyId` deve ser especificado no seguinte formato:

`projectId:location:keyRingName:cryptoKeyName`

Por exemplo, se você quiser usar a chave `my-example-key` no anel de chaves `my-example-key-ring` na região `us-east1` e no projeto com ID `my-example-project-1`, suas configurações personalizadas `ProvScheme` seriam semelhantes a:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />

</CustomProperties>'
```

Todos os discos e imagens provisionados pelo MCS relacionados a este esquema de provisionamento usam esta chave de criptografia gerenciada pelo cliente.

> **Dica:**

> Se você usar chaves globais, o local das propriedades do cliente deve dizer `global` e não o nome da **região**, que no exemplo acima é **us-east1**. Por exemplo: `<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`.

Criar um catálogo de máquinas usando um perfil de máquina

Ao criar um catálogo para provisionar máquinas usando o Machine Creation Services (MCS), você pode usar um perfil de máquina para capturar as propriedades de hardware de uma máquina virtual e aplicá-las às VMs recém-provisionadas no catálogo. Quando o parâmetro `MachineProfile` não é usado, as propriedades de hardware são capturadas da VM da imagem mestre ou do snapshot. Algumas propriedades que você define explicitamente, por exemplo, `StorageType`, `CatalogZones` e `CryptoKeyId`, são ignoradas do perfil da máquina.

- Para criar um catálogo com um perfil de máquina, use o comando `New-ProvScheme`. Por exemplo, `New-ProvScheme –MachineProfile “path to VM”`. Se você não especificar o parâmetro `MachineProfile`, as propriedades de hardware serão capturadas da VM da imagem mestre.
- Para atualizar um catálogo com um novo perfil de máquina, use o comando `Set-ProvScheme`. Por exemplo, `Set-ProvScheme –MachineProfile “path to new VM”`. Este comando não altera o perfil de máquina das VMs existentes no catálogo. Somente as VMs recém-criadas adicionadas ao catálogo terão o novo perfil de máquina.
- Você também pode atualizar a imagem mestre, no entanto, ao atualizar a imagem mestre, as propriedades de hardware não são atualizadas. Se você quiser atualizar as propriedades de hardware, você precisa atualizar o perfil da máquina usando o comando `Set-ProvScheme`. Essas alterações só se aplicarão às novas máquinas no catálogo. Para atualizar as propriedades de hardware de uma máquina existente, você pode usar o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`.

  > **Nota:**
  >
  > - `StartsNow` indica que a hora de início agendada é a hora atual.
  > - `DurationInMinutes` com um número negativo (por exemplo, –1) indica que não há limite superior para a janela de tempo do agendamento.

Criar um catálogo de máquinas com perfil de máquina como um modelo de instância

Você pode selecionar um modelo de instância do GCP como entrada para o perfil da máquina. Os modelos de instância são recursos leves no GCP e, portanto, são muito econômicos.

Criar um novo catálogo de máquinas com perfil de máquina como um modelo de instância

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Encontre um modelo de instância em seu projeto GCP usando o seguinte comando:

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. Crie um novo catálogo de máquinas com perfil de máquina como um modelo de instância usando o comando NewProvScheme:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName>\Base.vm\Base.snapshot
-MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

   Para obter mais informações sobre o comando New-ProvScheme, consulte `<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/>`.

5. Conclua a criação do catálogo de máquinas usando comandos do PowerShell.

Atualizar um catálogo de máquinas para ter um modelo de instância como perfil de máquina

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

Para obter informações sobre o comando Set-ProvScheme, consulte `<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/>`.

Criar um catálogo com VM blindada

Você pode criar um catálogo de máquinas MCS com propriedades de VM blindada. Uma máquina virtual blindada é reforçada por um conjunto de controles de segurança que fornecem integridade verificável de suas instâncias do Compute Engine, usando recursos avançados de segurança da plataforma, como inicialização segura, um módulo de plataforma confiável virtual, firmware UEFI e monitoramento de integridade.

O MCS oferece suporte à criação do catálogo usando o fluxo de trabalho de perfil de máquina. Se você usar o fluxo de trabalho de perfil de máquina, deverá habilitar as propriedades de VM blindada de uma instância de VM. Você pode então usar esta instância de VM como entrada de perfil de máquina.

Criar um catálogo de máquinas MCS com VM blindada

1. Habilite as opções de VM blindada de uma instância de VM no console do Google Cloud. Consulte Início rápido: Habilitar opções de VM blindada.
2. Crie um catálogo de máquinas MCS com fluxo de trabalho de perfil de máquina usando a instância de VM.
    a. Abra uma janela do PowerShell
    b. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
    c. Crie um pool de identidades se ainda não tiver sido criado.
    d. Execute o comando `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>

-HostingUnitName gcp-hostint-unit

-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm
```

```
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
machine.vm
```

3. Conclua a criação do catálogo de máquinas.

Atualizar um catálogo de máquinas com um novo perfil de máquina

1. Execute o comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>

-MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

-MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
```

Para aplicar a alteração feita em `Set-ProvScheme` às VMs existentes, execute o comando `Set-ProvVMUpdateTimeWindow`.

1. Execute o comando `Set-ProvVMUpdateTimeWindow`. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. Reinicie as VMs.

Criar VMs do Windows 11 no nó de locatário único

Você pode criar VMs do Windows 11 no GCP. No entanto, se você instalar o Windows 11 na imagem mestre, deverá habilitar o vTPM durante o processo de criação da imagem mestre. Além disso, você deve habilitar o vTPM na origem do perfil da máquina (VM ou modelo de instância).

As principais etapas para criar VMs do Windows 11 no nó de locatário único são:

1. Configure os ambientes de virtualização do Google Cloud. Para obter informações, consulte Ambientes do Google Cloud.
2. Instale o VDA. Consulte Instalar VDAs.
3. Crie uma conexão com os ambientes do Google Cloud. Para obter informações, consulte Conexão com ambientes do Google Cloud.
4. Crie uma imagem mestre do Windows 11 Bring Your Own License (BYOL) e importe a imagem para o Google Cloud. Consulte Criar uma imagem mestre BYOL do Windows 11.

5. Crie a origem do perfil da máquina: Provisione a VM no nó de locatário único e habilite o vTPM do perfil da máquina de origem. Consulte Provisionar VM no nó de locatário único.
6. Crie um catálogo de máquinas MCS usando a origem do perfil da máquina do Windows 11 habilitada com vTPM. A origem do perfil da máquina deve ter o mesmo tipo de instância descrito no nó de locatário único. Consulte Criar um catálogo de máquinas MCS usando a origem do perfil da máquina do Windows 11.

Criar uma imagem mestre BYOL do Windows 11

Existem duas opções para criar uma imagem mestre BYOL do Windows 11 e importar a imagem mestre para o Google Cloud:

- Usar as Ferramentas de Compilação do Google Cloud
- Criar a imagem mestre em qualquer outro hipervisor

USAR AS FERRAMENTAS DE COMPILAÇÃO DO GOOGLE CLOUD

1. Carregue os arquivos ISO do Windows 11, GCP SDK, .NET framework e instalador do PowerShell para o bucket de armazenamento do GCP.
2. Forneça o local do arquivo no arquivo `.yaml` de compilação na nuvem como parâmetro.
3. Execute o seguinte Cloud Build a partir da linha de comando para criar a imagem final do Windows 11. O GCP inicializa e cria a imagem mestre no projeto selecionado usando o fluxo de trabalho Daisy no GCP, e a imagem mestre é importada para o GCP.

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **Nota:**
>
> Substitua todo o texto em letras maiúsculas pelos detalhes reais do recurso.

Para obter informações completas, consulte Criar imagens BYOL personalizadas do Windows.

CRIAR A IMAGEM MESTRE EM QUALQUER OUTRO HIPERVISOR

1. Crie a imagem mestre do Windows 11 usando qualquer outro hipervisor.
2. Exporte a imagem mestre em formato OVF para a máquina local.

3. Carregue os arquivos OVF para o bucket de armazenamento do GCP usando a CLI gcloud local.

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. Execute o seguinte Cloud Build a partir da linha de comando para criar a imagem final do Windows 11. O GCP inicializa e cria a imagem mestre no projeto selecionado usando o fluxo de trabalho Daisy no GCP, e a imagem mestre é importada para o GCP.

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **Nota:**
>
> Substitua todo o texto em letras maiúsculas pelos detalhes reais do recurso.

Provisionar VM em nó de locatário único

Use nós de locatário único para manter suas VMs fisicamente separadas de VMs em outros projetos, ou para agrupar suas VMs no mesmo hardware de host. Para obter informações sobre o nó de locatário único, consulte o documento do GCP Visão geral da locação única.

Para provisionar uma VM (origem do perfil da máquina) no nó de locatário único, consulte o documento do GCP Provisionar VMs em nós de locatário único.

> **Nota:**
>
> - Selecione o mesmo tipo de instância e região que o grupo de nós.
> - Habilite o vTPM na seção VM Blindada. Para obter mais informações, consulte Início rápido: Habilitar opções de VM Blindada.
> - Desative o Bitlocker na VM de origem.

Criar um catálogo de máquinas MCS usando a origem do perfil de máquina do Windows 11

Você pode criar um catálogo de máquinas MCS para criar VMs do Windows 11 usando o Studio ou comandos do PowerShell.

Nota:

- Para a imagem mestre, selecione o Snapshot ou a VM do Windows 11.
- Para a origem do perfil da máquina, selecione a VM do Windows 11 como perfil da máquina. A origem do perfil da máquina deve ter o mesmo tipo de instância descrito no nó de locatário único.

Para obter informações sobre como usar o Studio, consulte Criar um catálogo de máquinas usando o Studio.

Para obter informações sobre comandos do PowerShell, consulte Criar um catálogo de máquinas usando um perfil de máquina.

Depois de criar o catálogo e ligar as VMs, você pode ver as VMs do Windows 11 sendo executadas no nó de locatário único no console do Google Cloud.

VMs e discos com rótulos herdados

As VMs e discos do catálogo de máquinas MCS (Disco de Identidade, Disco de Retorno de Cache de Gravação e disco do SO) podem herdar os rótulos de uma fonte de perfil de máquina (instância de VM GCP ou modelo de instância). Você pode usar os rótulos para distinguir instâncias pertencentes a diferentes equipes (por exemplo, team:research e team:analytics) e usá-los ainda mais para contabilidade de custos ou orçamento. Para obter mais informações sobre rótulos, consulte o documento do GCP Organizar recursos usando rótulos.

Você pode criar um novo catálogo, atualizar um catálogo existente e atualizar VMs existentes para herdar os rótulos usando a fonte do perfil da máquina.

Este recurso é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

Você pode fazer o seguinte:

- Criar um catálogo com rótulos herdados
- Atualizar um catálogo existente com rótulos herdados

- Atualizar VMs existentes com rótulos herdados
- Recuperar informações para rótulos de VM e disco de inicialização
- Remover uma VM

Criar um catálogo com rótulos herdados

Para criar um catálogo de máquinas MCS onde VMs e discos herdam rótulos da fonte do perfil da máquina, faça o seguinte:

1. Crie uma fonte de perfil de máquina (instância de VM ou modelo de instância) com rótulos. Para obter informações sobre como criar VMs com rótulos, consulte o documento do GCP Criar recursos com rótulos. Um modelo de instância é criado a partir da VM e assume os rótulos definidos na VM.
2. Crie um catálogo MCS usando o Studio ou comandos PowerShell.
3. Se estiver usando o Studio, na página **Imagem**, selecione **Usar um perfil de máquina** e, em seguida, selecione a VM ou o modelo.
4. Se estiver usando comandos do PowerShell, faça o seguinte:
    a. Abra a janela do PowerShell.
    b. Execute asnp citrix*.
    c. Crie um pool de identidades. O pool de identidades é um contêiner para as contas do Active Directory (AD) das VMs a serem criadas.
    d. Crie as contas de computador AD necessárias no Active Directory.
    e. Execute o comando `New-ProvScheme` para criar um catálogo. Por exemplo:

    New-ProvScheme com modelo como entrada de perfil de máquina (Catálogo persistente):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

```
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

New-ProvScheme com modelo de instância como entrada de perfil de máquina (Catálogo não persistente):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `

-CleanOnBoot
```

New-ProvScheme com instância de VM como entrada de perfil de máquina (Catálogo persistente):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

New-ProvScheme com instância de VM como entrada de perfil de máquina (Catálogo não persistente):

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-CleanOnBoot
```

f. Registre o esquema de provisionamento como um catálogo de broker.

g. Adicione VMs ao catálogo.

Atualizar um catálogo existente com rótulos herdados

Para atualizar um catálogo existente para ter um novo perfil de máquina, execute o comando Set-ProvScheme. Depois de executar o comando, todas as novas VMs adicionadas ao catálogo terão os rótulos da nova origem do perfil de máquina. O catálogo não persistente é atualizado na próxima inicialização.

Por exemplo:

Set-ProvScheme com modelo de instância como entrada de perfil de máquina:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

Set-ProvScheme com instância de VM como entrada de perfil de máquina:

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `
```

```
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

Atualizar VMs existentes com rótulos herdados

Para atualizar as VMs existentes com a fonte de perfil de máquina atualizada, execute os seguintes comandos:

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`. Por exemplo:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

3. Reinicie as VMs.

Recuperar informações para rótulos de VM e disco de inicialização

Após criar as VMs, você pode obter as informações do rótulo da VM e do disco de inicialização usando o comando `Get-Item` com o parâmetro `AdditionalData`.

Para recuperar informações do rótulo da VM, execute o seguinte comando:

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-
name\vm_name.vm).AdditionalData.Tags
```

Para recuperar informações do rótulo do disco de inicialização, execute o seguinte comando:

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
name.attacheddisk).AdditionalData.Tags
```

Nota:

Para manter a consistência entre os vários hipervisores, usamos o termo Tags para exibir os rótulos do GCP.

Remover uma VM

Você pode optar por remover uma VM de um catálogo, mas não excluir a VM do GCP. Neste caso, os rótulos Citrix são removidos apenas da VM. Todos os outros rótulos adicionados não são excluídos da VM. Você pode remover uma VM do Studio ou usar comandos PowerShell.

USANDO O STUDIO

1. Selecione e clique com o botão direito do mouse na VM.
2. Clique em **Excluir**.
3. Selecione **Remover as máquinas virtuais do catálogo, mas não excluir as máquinas virtuais**.

USANDO COMANDOS POWERSHELL

Execute `Remove-ProvVM` com o parâmetro `ForgetVM`. Para obter mais informações, consulte a documentação do SDK Remove-ProvVM.

Google Cloud Marketplace

Você pode procurar e selecionar imagens oferecidas pela Citrix no Google Cloud Marketplace para criar catálogos de máquinas. Atualmente, o MCS suporta apenas o fluxo de trabalho de perfil de máquina para este recurso.

Para pesquisar o produto Citrix VDA VM através do Google Cloud Marketplace, acesse `<https://console.cloud.google.com/marketplace/>`.

Você pode usar uma imagem personalizada ou uma imagem Citrix ready® no Google Cloud Marketplace para atualizar uma imagem de um catálogo de máquinas.

> **Nota:**

> Se o perfil da máquina não contiver informações de tipo de armazenamento, o valor será derivado das propriedades personalizadas.

> As imagens suportadas do Google Cloud Marketplace são:

- Windows 2019 Single Session
- Windows 2019 Multissessão
- Ubuntu

Exemplo de uso de uma imagem pronta para Citrix como fonte para criar um catálogo de máquinas:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

Próximos passos

- Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.
- Para revisar todo o processo de configuração, consulte Planejar e construir uma implantação.
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Google Cloud Platform.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com ambientes de nuvem do Google
- Criar catálogos de máquinas

Criar um catálogo de máquinas HPE Moonshot

(/pt-br/citrix-daas/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes HPE Moonshot.

Nota:

- Criar uma conexão com o HPE Moonshot
- Certifique-se de ter um ou mais nós HPE Moonshot disponíveis e instale VDAs nesses nós.

> - Para obter informações sobre como criar a imagem inicial do cartucho HPE Moonshot, consulte o Guia do Usuário de Implantação de SO no Moonshot.

> Você pode criar um catálogo de máquinas HPE Moonshot usando:

- Studio
- Comandos PowerShell

Criar um catálogo de máquinas usando o Studio

No assistente de **Configuração do Catálogo de Máquinas**:

1. Na página **Sistema Operacional**, selecione **SO multissessão** ou **SO de sessão única**.
2. Na página **Gerenciamento de Máquinas**, selecione **Máquinas com gerenciamento de energia** e **Outro serviço ou tecnologia**.
3. Na página **Máquinas Virtuais**, adicione máquinas e suas contas de máquina do Active Directory. Você pode fazer uma das seguintes opções:
   - Clique em **Adicionar Máquinas** para adicionar máquinas manualmente. A janela **Selecionar VMs** é exibida. Expanda a conexão do chassi HPE Moonshot que você criou anteriormente e selecione os nós (VMs) que deseja adicionar. Em seguida, adicione os nomes das contas de máquina associadas.
   - Clique em **Adicionar Arquivo CSV** para adicionar máquinas em massa. Para obter informações sobre como usar arquivos CSV para adicionar máquinas, consulte Usar arquivos CSV para adicionar máquinas em massa a um catálogo.

As páginas **Escopos** e **Resumo** não contêm informações específicas do HPE Moonshot.

Criar um catálogo de máquinas usando comandos PowerShell

Execute os comandos PowerShell `New-BrokerCatalog` e `New-BrokerMachine` para criar um catálogo de broker e importar máquinas para o catálogo de broker.

Por exemplo:

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"
```

```
New-BrokerMachine -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

Onde ir em seguida

- Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.
- Para revisar todo o processo de configuração, consulte Planejar e construir uma implantação.
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo HPE Moonshot.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com HPE Moonshot
- Criar catálogos de máquinas

Criar um catálogo do Microsoft Azure

(/pt-br/citrix-daas/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de nuvem do Microsoft Azure Resource Manager.

Nota:

Antes de criar um catálogo do Microsoft Azure, você precisa concluir a criação de uma conexão com o Microsoft Azure. Consulte Conexão com o Microsoft Azure.

Criar um catálogo de máquinas

Você pode criar um catálogo de máquinas de duas maneiras:

- Studio.
- PowerShell. Consulte Gerenciar Citrix DaaS usando SDKs remotos do PowerShell. Para obter informações sobre como implementar recursos específicos usando o PowerShell, consulte Usar PowerShell.

Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Studio

Esta informação é um suplemento às orientações em Criar catálogos de máquinas.

Uma imagem pode ser um disco, um instantâneo ou uma versão de imagem de uma definição de imagem dentro da Galeria de Computação do Azure que é usada para criar as VMs em um catálogo de máquinas.

Antes de criar o catálogo de máquinas, crie uma imagem no Azure Resource Manager.

Nota:

- O uso de disco não gerenciado para provisionar VM foi descontinuado.
- O suporte para usar uma imagem mestre de uma região diferente da configurada na conexão do host foi descontinuado. Use a Galeria de Computação do Azure para replicar a imagem mestre para a região desejada.

Ao criar um catálogo de máquinas MCS, uma VM temporária é criada com base na VM original para executar tarefas de preparação, como habilitar DHCP e rearmar a licença. Essa VM temporária é chamada de VM de preparação. O nome dessa VM de preparação segue o formato **Preparati-84x9n**, onde os últimos cinco caracteres são gerados aleatoriamente para evitar duplicação. A convenção de nomenclatura para essa VM de preparação é fixa e não pode ser personalizada. Após a conclusão das tarefas de preparação, a VM de preparação é destruída.

Para desconectar a rede da VM de preparação, um grupo de segurança de rede é criado para negar todo o tráfego de entrada e saída. O grupo de segurança de rede é criado automaticamente uma vez por catálogo. O nome do grupo de segurança de rede é `Citrix-Deny-All-a3pgu-GUID`, onde GUID é gerado aleatoriamente. Por exemplo, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

No assistente de criação de catálogo de máquinas:

1. As páginas **Tipo de Máquina** e **Gerenciamento de Máquinas** não contêm informações específicas do Azure. Siga as orientações no artigo Criar catálogos de máquinas.

2. Na página **Imagem**, selecione uma imagem que você deseja usar como imagem mestre para todas as máquinas no catálogo. O assistente **Selecionar uma imagem** é exibido. Siga estas etapas para selecionar uma imagem:

   a. (Aplicável apenas a conexões configuradas com imagens compartilhadas dentro ou entre locatários) Selecione uma assinatura onde a imagem reside.

   b. Selecione um grupo de recursos.

   c. navegar para o disco gerenciado do Azure, Azure Compute Gallery ou versão da imagem do Azure.

   Ao selecionar uma imagem, considere o seguinte:

   - Verifique se um Citrix VDA está instalado na imagem.
   - Se você selecionar um disco anexado a uma VM, deverá desligar a VM antes de prosseguir para a próxima etapa.

> **Nota:**
>
> - A assinatura correspondente à conexão (host) que criou as máquinas no catálogo é indicada com um ponto verde. As outras assinaturas são aquelas que têm a Azure Compute Gallery compartilhada com essa assinatura. Nessas assinaturas, apenas galerias compartilhadas são mostradas. Para obter informações sobre como configurar assinaturas compartilhadas, consulte Compartilhar imagens dentro de um locatário (entre assinaturas) e Compartilhar imagens entre locatários.
> - Você pode criar um esquema de provisionamento usando disco de SO efêmero no Windows com Trusted Launch. Ao selecionar uma imagem com Trusted Launch, você deve selecionar um perfil de máquina com Trusted Launch que esteja habilitado com vTPM. Para criar catálogos de máquinas usando disco de SO efêmero, consulte Como criar máquinas usando discos de SO efêmeros.
> - Quando a replicação da imagem estiver em andamento, você pode prosseguir e selecionar a imagem como imagem mestre e concluir a configuração. No entanto, a criação do catálogo pode levar mais tempo para ser concluída enquanto a imagem está sendo replicada. O MCS exige que a replicação seja concluída em uma hora a partir da criação do catálogo. Se a replicação expirar, a criação do catálogo falhará. Você pode verificar o status da replicação no Azure. Tente novamente se a replicação ainda estiver pendente ou após a conclusão da replicação.

- Você pode provisionar um catálogo de VMs Gen2 usando uma imagem Gen2 para melhorar o desempenho do tempo de inicialização. No entanto, a criação de um catálogo de máquinas Gen2 usando uma imagem Gen1 não é suportada. Da mesma forma, a criação de um catálogo de máquinas Gen1 usando uma imagem Gen2 também não é suportada. Além disso, qualquer imagem mais antiga que não tenha informações de geração é uma imagem Gen1.

Escolha se deseja que as VMs no catálogo herdem as configurações de um perfil de máquina. Por padrão, a caixa de seleção **Usar um perfil de máquina (obrigatório para Microsoft Entra ID)** é selecionada. Clique em **Selecionar um perfil de máquina** para procurar uma VM ou uma especificação de modelo ARM em uma lista de grupos de recursos.

Exemplos de configurações que as VMs podem herdar de um perfil de máquina incluem:

- Rede acelerada
- Diagnóstico de inicialização
- Cache de disco do host (relacionado a discos de SO e MCSIO)
- Tamanho da máquina (salvo especificação em contrário)
- Tags colocadas na VM

Nota:

- Ao selecionar uma imagem mestre para catálogos de máquinas no Azure, o perfil da máquina é filtrado com base na imagem mestre selecionada. Por exemplo, o perfil da máquina é filtrado com base no SO Windows, tipo de segurança, suporte à hibernação e ID do conjunto de criptografia de disco da imagem mestre.
- O uso de um perfil de máquina com Inicialização Confiável como **Tipo de Segurança** é obrigatório ao selecionar uma imagem ou instantâneo que tenha a Inicialização Confiável habilitada. Você pode então habilitar ou desabilitar o SecureBoot e o vTPM especificando seus valores no Perfil da Máquina. Para obter informações sobre a Inicialização Confiável do Azure, consulte `<https://docs.microsoft.com/pt-br/azure/virtual-machines/trusted-launch>`.

> Valide a especificação do modelo ARM para garantir se ela pode ser usada como um perfil de máquina para criar um catálogo de máquinas. Para obter informações sobre como criar uma especificação de modelo do Azure, consulte Criar uma especificação de modelo do Azure.

Existem duas maneiras de validar a especificação do modelo ARM:

- Depois de selecionar a especificação do modelo ARM na lista de grupos de recursos, clique em **Avançar**. Mensagens de erro aparecerão se a especificação do modelo ARM tiver erros.
- Execute um dos seguintes comandos do PowerShell:
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

  Por exemplo:

```
Test-ProvInventoryItem -HostingUnitName "we-vdi0101-d-vnet"
-InventoryPath machineprofile.folder/vdi01-d-rg.resourcegroup/VDD-
templ-spec.templatespec/1.5.templatespecversion
```

Depois de criar o catálogo, você pode visualizar as configurações que a imagem herda do perfil da máquina. No nó **Catálogos de Máquinas**, selecione o catálogo para visualizar seus detalhes no painel inferior. Em seguida, clique na guia **Propriedades do Modelo** para visualizar as propriedades do perfil da máquina. A seção **Tags** exibe até três tags. Para visualizar todas as tags colocadas na VM, clique em **Visualizar tudo**.

Se você quiser que o MCS provisione VMs em um host dedicado do Azure, habilite a caixa de seleção **Usar um grupo de hosts** e selecione um grupo de hosts na lista. Um grupo de hosts é um recurso que representa uma coleção de hosts dedicados. Um host dedicado é um serviço que fornece servidores físicos que hospedam uma ou mais máquinas virtuais. Seu servidor é dedicado à sua assinatura do Azure, não compartilhado com outros assinantes. Ao usar um host dedicado, o Azure garante que suas VMs sejam as únicas máquinas em execução nesse host. Esse recurso é adequado para cenários em que você deve atender a requisitos regulatórios ou de segurança interna. Para saber mais sobre grupos de hosts e considerações para usá-los, consulte Provisionar VMs em hosts dedicados do Azure.

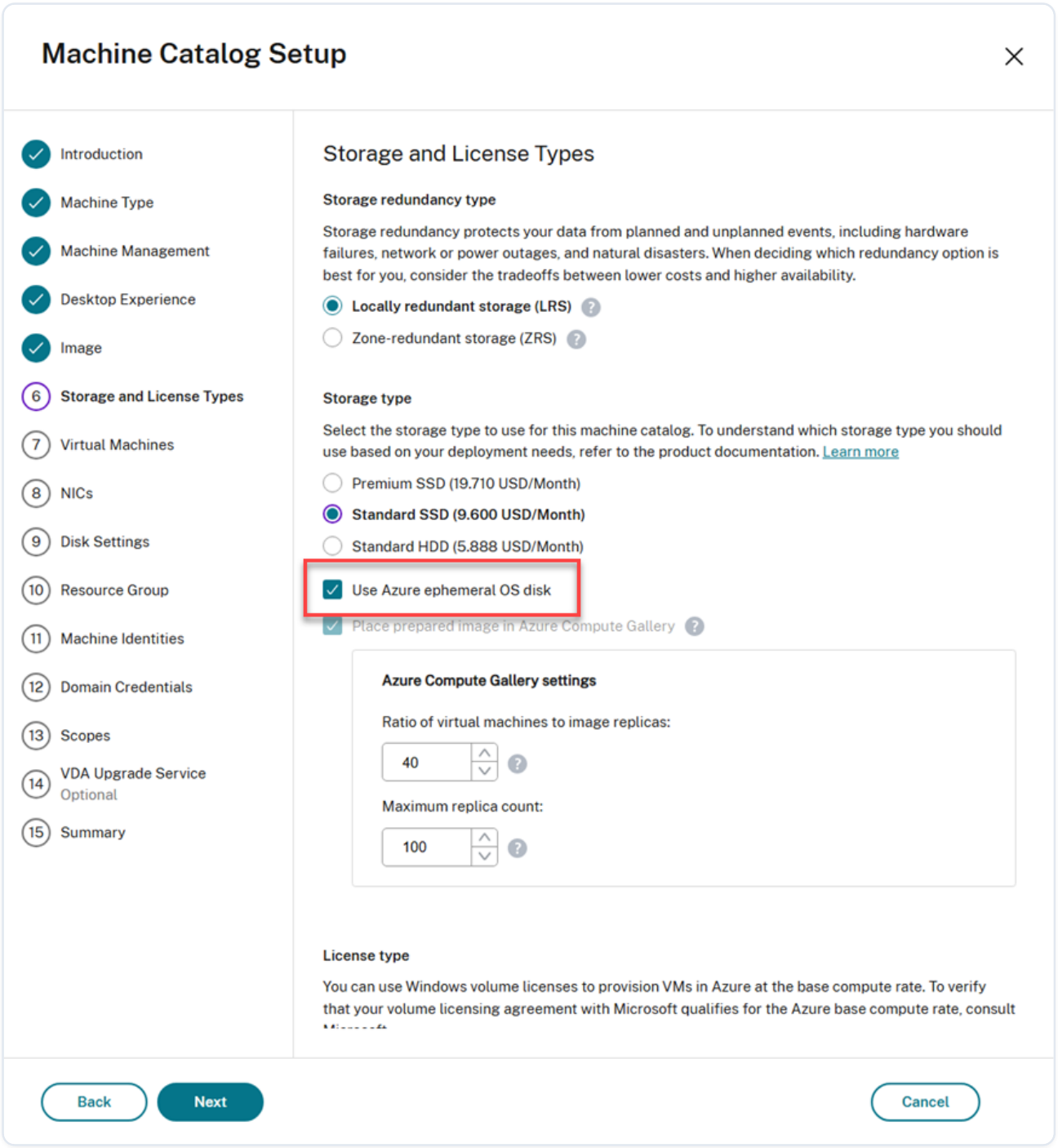
> **Importante:**

- Somente os grupos de hosts que têm o posicionamento automático do Azure habilitado são exibidos.
- O uso de um grupo de hosts altera a página **Máquinas Virtuais** oferecida posteriormente no assistente. Somente os tamanhos de máquina que o grupo de hosts selecionado contém são exibidos nessa página. Além disso, as Zonas de Disponibilidade são selecionadas automaticamente e não estão disponíveis para seleção.

3. A página **Tipos de Armazenamento e Licença** aparece somente quando você usa uma imagem do Azure Resource Manager.

   - Selecione o **Tipo de redundância de armazenamento**:
     - Armazenamento com redundância local (LRS): O LRS permite que você escolha entre todos os tipos de armazenamento disponíveis. Ao usar o LRS, o Azure implanta as Máquinas Virtuais (VMs) exclusivamente dentro da zona de disponibilidade especificada.
     - Armazenamento com redundância de zona (ZRS): O ZRS permite maior flexibilidade no posicionamento de VMs, pois o Azure pode iniciar VMs em qualquer zona disponível. Esta é uma vantagem fundamental sobre o Armazenamento com Redundância Local (LRS), garantindo a disponibilidade da VM mesmo que a zona original do disco se torne inacessível. O ZRS, no entanto, é compatível apenas com os tipos de armazenamento Premium SSD e Standard SSD.
   - Selecione os **Tipos de armazenamento** a serem usados para o catálogo de máquinas: O tipo de armazenamento determina quais tamanhos de máquina são oferecidos na página **Máquinas Virtuais** do assistente.
     - **SSD Premium**. Oferece uma opção de armazenamento em disco de alto desempenho e baixa latência, adequada para VMs com cargas de trabalho intensivas em E/S.
     - **SSD Standard**. Oferece uma opção de armazenamento econômica que é adequada para cargas de trabalho que exigem desempenho consistente em níveis de IOPS mais baixos.
     - **Standard HDD**. Oferece uma opção de armazenamento em disco confiável e de baixo custo, adequada para VMs que executam cargas de trabalho insensíveis à latência.

- Selecione **Usar disco de SO efêmero do Azure**. O disco de SO efêmero do Azure oferece uma opção de armazenamento econômica que reutiliza o disco local das VMs para hospedar o disco do sistema operacional. Como alternativa, você pode usar o PowerShell para criar máquinas que usam discos de SO efêmeros. Para obter mais informações, consulte Discos efêmeros do Azure. Considere o seguinte ao usar um disco de SO efêmero:
  - O disco de SO efêmero do Azure e o MCS I/O não podem ser habilitados ao mesmo tempo.
  - Para atualizar máquinas que usam discos de SO efêmeros, você deve selecionar uma imagem cujo tamanho não exceda o tamanho do disco de cache ou do disco temporário da VM.
  - Você não pode usar a opção **Manter VM e disco do sistema durante ciclos de energia** oferecida posteriormente no assistente.



Nota:

- O disco de identidade é sempre criado usando SSD Standard, independentemente do tipo de armazenamento escolhido.
- Se você selecionar **ZRS** como **Redundância de armazenamento**, você terá a opção de selecionar apenas **Premium SSD** e **Standard SSD**.

For details about Azure storage types and storage replication, see the following:

- [Introduction to Azure Storage](https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/)

- [Azure premium storage: Design for high performance](https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/)

- [Azure Storage redundancy](https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/)

Select whether to use existing Windows licenses or Linux licenses:

- Windows licenses: Using Windows licenses along with Windows images (Azure platform support images or custom images) lets you run Windows VMs in Azure at a reduced cost. There are two types of licenses:

    - **Windows Server license**. Lets you use your Windows Server or Azure Windows Server licenses, allowing you to use Azure Hybrid Benefits. For details, see `<https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>`. Azure Hybrid Benefit reduces the cost of running VMs in Azure to the base compute rate, waiving the cost of extra Windows Server licenses from the Azure gallery.

    - **Windows Client license**. Lets you bring your Windows 10 and Windows 11 licenses to Azure, allowing you to run Windows 10 and Windows 11 VMs in Azure without the need for extra licenses. For details, see [Client Access Licenses and Management Licenses](https://www.microsoft.com/en-us/licensing/product-licensing/client-access-license).

- Linux licenses: With bring-your-own-subscription (BYOS) Linux licenses, you do not have to pay for the software. The BYOS charge only includes the compute hardware fee. There are two types of licenses:

    - **RHEL_BYOS**: To use RHEL_BYOS type successfully, enable Red Hat Cloud Access on your Azure subscription.

    - **SLES_BYOS**: The BYOS versions of SLES include support from SUSE.

See the following:

- [Verify the Windows license](#verificar-a-licença-do-windows)

- [Configure the Linux license](#configurar-a-licença-do-linux)

See the following documents to understand License types and their benefits:

- `<https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`

- `<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

Azure Compute Gallery is a repository for managing and sharing images. It lets you make your images available throughout your organization. We recommend that you store an image in Azure Compute Gallery when creating

```
large non-persistent machine catalogs because doing that enables faster
resets of VDA OS disks. After you select **Place prepared image in Azure
Compute Gallery**, the **Azure Compute Gallery settings** section appears,
letting you specify more Azure Computer Gallery settings:



-  **Ratio of virtual machines to image replicas**. Lets you specify the
ratio of virtual machines to image replicas that you want Azure to keep.
By default, Azure keeps a single image replica for every 40 non-persistent
machines. For persistent machines, that number defaults to 1,000.



-  **Maximum replica count**. Lets you specify the maximum number of image
replicas that you want Azure to keep. The default is 100.



For information on Azure Compute Gallery, see [Azure Compute Gallery]
(#galeria-de-computação-do-azure).



> **Note:**

>

> A gallery is created in ACG to store the image. This gallery is
accessible only to MCS for VM creation and doesn't appear on the **Select
an image** page.
```

1. Na página **Máquinas Virtuais**, indique quantas VMs você deseja criar e o tamanho da máquina. Após a criação do catálogo, você pode alterar o tamanho da máquina editando o catálogo.

   Agora você pode configurar uma VM secundária quando o tamanho da máquina primária atingir a capacidade total. Para configurar tamanhos de VM secundários, clique em **Tamanho secundário (opcional)**.

   a. Na janela **Tamanho da máquina secundária**, as VMs listadas têm tipos de VM Spot e Regular. Você pode selecionar até 10 tamanhos de máquinas secundárias. Uma vez que as 10 VMs são selecionadas, as outras VMs listadas são desabilitadas para seleção futura.

b. Clique em **Avançar**. No painel **Tamanho da máquina secundária**, você pode selecionar vários tamanhos de máquina e arrastar e soltar para alterar a ordem de prioridade. Clique em **Concluído**. Os tamanhos de máquina selecionados aparecem em **Tamanho secundário (opcional)**. Clique no ícone de edição para editar conforme necessário.

Nota:

- Se a propriedade Tamanho do Disco Temporário estiver definida para uma VM primária, somente as VMs secundárias com a propriedade Tamanho do Disco Temporário definida serão listadas.
- Se a propriedade Tamanho do Disco Temporário não estiver definida para uma VM primária, as VMs secundárias sem a propriedade Tamanho do Disco Temporário serão listadas.
- Se você modificar a VM primária, deverá reconfigurar a VM secundária.
- Perfis de máquina são obrigatórios para tamanhos de máquina secundários.
- Os tamanhos de VM secundários que não suportam spot são mostrados apenas quando uma das seguintes condições é atendida; caso contrário, todos os tamanhos de VM secundários são mostrados:
- O tamanho da VM primária não suporta spot
- O tamanho da VM primária suporta spot, mas o MP não suporta spot
- O perfil da máquina suporta hibernação

2. A página **NICs** não contém informações específicas do Azure. Siga as orientações no artigo Criar catálogos de máquinas.
3. Na página **Configurações de Disco**, escolha se deseja habilitar o cache de write-back. Com o recurso de otimização de armazenamento do MCS habilitado, você pode configurar as seguintes configurações ao criar um catálogo.

   Após habilitar o cache de write-back, você pode fazer o seguinte:

   - Configure o tamanho do disco e da RAM usados para armazenar dados temporários em cache. Para obter mais informações, consulte Configurar cache para dados temporários.
   - Selecione o tipo de armazenamento para o disco de cache de write-back. As seguintes opções de armazenamento estão disponíveis para uso no disco de cache de write-back:

- SSD Premium
- SSD Standard
- HDD Standard

> **Nota:**
>
> Se você selecionar **ZRS** como **Redundância de armazenamento** na página **Tipos de armazenamento e licença**, a redundância de armazenamento do disco de cache de write-back será definida como ZRS por padrão.

- Escolha se deseja que o disco de cache de write-back persista para as VMs provisionadas. Selecione **Habilitar cache de write-back** para disponibilizar as opções. Por padrão, **Usar disco de cache de write-back não persistente** é selecionado.
- Selecione o tipo para o disco de cache de write-back.
  - **Usar disco de cache de write-back não persistente**. Se selecionado, o disco de cache de write-back é excluído durante os ciclos de energia. Quaisquer dados redirecionados para ele serão perdidos. Se o disco temporário da VM tiver espaço suficiente, ele será usado para hospedar o disco de cache de write-back para reduzir seus custos. Após a criação do catálogo, você pode verificar se as máquinas provisionadas usam o disco temporário. Para fazer isso, clique no catálogo e verifique as informações na guia **Propriedades do Modelo**. Se o disco temporário for usado, você verá **Disco de Cache de Write-back Não Persistente** e seu valor será **Sim (usando o disco temporário da VM)**. Caso contrário, você verá **Disco de Cache de Write-back Não Persistente** e seu valor será **Não (não usando o disco temporário da VM)**.
  - **Usar disco de cache de write-back persistente**. Se selecionado, o disco de cache de write-back persiste para as VMs provisionadas. Habilitar a opção aumenta seus custos de armazenamento.

> **Nota:**
>
> Um catálogo usa automaticamente o Disco Temporário do Azure para o disco WBC se todos os seguintes critérios forem atendidos:

- MCSIO está habilitado.
- O disco WBC não é persistente.
- O tamanho da VM inclui um Disco Temporário grande o suficiente para o disco WBC.
- Nenhuma letra de unidade é especificada para o disco WBC. Este recurso se aplica tanto à criação quanto à edição de catálogos, ajudando a reduzir seus custos de armazenamento.

- Escolha se deseja reter VMs e discos de sistema para VDAs durante os ciclos de energia.

  Reter VM e disco de sistema durante os ciclos de energia. Disponível quando você selecionou **Habilitar cache de write-back**. Por padrão, as VMs e os discos de sistema são excluídos no desligamento e recriados na inicialização. Se você deseja reduzir os tempos de reinicialização da VM, selecione esta opção. Lembre-se de que habilitar esta opção também aumenta os custos de armazenamento.

- Escolha se deseja **Habilitar economia de custos de armazenamento**. Se habilitado, economize custos de armazenamento fazendo o downgrade do disco de armazenamento para HDD Padrão quando a VM for desligada. A VM retorna às suas configurações originais na reinicialização. A opção se aplica a discos de armazenamento e de cache de write-back. Alternativamente, você também pode usar o PowerShell. Consulte Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada.

  Nota:

  A Microsoft impõe restrições à alteração do tipo de armazenamento durante o desligamento da VM. Também é possível que a Microsoft bloqueie futuras alterações de tipo de armazenamento. Para obter mais informações, consulte este artigo da Microsoft.

- Escolha se deseja criptografar dados nas máquinas neste catálogo e qual chave de criptografia usar. A criptografia do lado do servidor com uma chave gerenciada pelo cliente (CMK) permite gerenciar a criptografia no nível do disco gerenciado e proteger dados nas máquinas do catálogo. As configurações padrão são herdadas do perfil da máquina ou da imagem mestre, com o perfil tendo prioridade:

- Se você estiver usando um *perfil de máquina* com um *CMK*, a opção **Usar a seguinte chave para criptografar dados em cada máquina** é selecionada automaticamente e assume como padrão a chave do *perfil de máquina*.
- Se você estiver usando um *perfil de máquina* com uma Chave Gerenciada pela Plataforma (PMK) e a *imagem mestre* for criptografada com *CMK*, a opção **Usar a seguinte chave para criptografar dados em cada máquina** é selecionada automaticamente e assume como padrão a chave da imagem mestre.
- Se você *não* estiver usando um *perfil de máquina* e a *imagem mestre* for criptografada com *CMK*, a opção **Usar a seguinte chave para criptografar dados em cada máquina** é selecionada automaticamente e assume como padrão a chave da *imagem mestre*.

Para obter mais informações, consulte Criptografia do lado do servidor do Azure.

4. Na página **Grupo de Recursos**, escolha se deseja criar grupos de recursos ou usar grupos existentes.

   - Se você optar por criar grupos de recursos, selecione **Avançar**.
   - Se você optar por usar grupos de recursos existentes, selecione os grupos na lista **Grupos de Recursos de Provisionamento Disponíveis**.

   > **Nota:**
   >
   > Selecione grupos suficientes para acomodar as máquinas que você está criando no catálogo. Uma mensagem aparece se você escolher poucos. Você pode querer selecionar mais do que o mínimo exigido se planeja adicionar mais VMs ao catálogo posteriormente. Você não pode adicionar mais grupos de recursos a um catálogo depois que ele é criado.

   > Para obter mais informações, consulte Grupos de recursos do Azure.

5. Na página **Identidades da Máquina**, escolha um tipo de identidade e configure as identidades para as máquinas neste catálogo. Se você selecionar as VMs como **Microsoft Entra joined**, poderá adicioná-las a um grupo de segurança do Microsoft Entra. As etapas detalhadas são as seguintes:

   a. No campo **Tipo de identidade**, selecione **Microsoft Entra joined**.

b. Clique em **Selecionar conta de serviço** e selecione uma conta de serviço com a capacidade de **gerenciamento de grupo de segurança do Microsoft Entra**.

c. Clique em **Grupo de segurança do Microsoft Entra: Criar novo**.

> **Observação:**
>
> **Criar novo** fica esmaecido se a conta de serviço selecionada não tiver a capacidade de **gerenciamento de grupo de segurança do Microsoft Entra**.

d. Insira um nome de grupo e depois clique em **Criar**.

e. Para adicionar o grupo de segurança a um grupo de segurança atribuído, selecione **Ingressar em um grupo de segurança atribuído como membro** e depois clique em **Selecionar um grupo** para escolher um grupo atribuído para ingressar.

f. Insira o esquema de nomenclatura da conta de máquina para as VMs.

Após a criação do catálogo, o Citrix DaaS™ acessa o Azure usando a conta de serviço selecionada e cria o grupo de segurança e uma regra de associação dinâmica para o grupo. Com base na regra, as VMs com o esquema de nomenclatura especificado neste catálogo são adicionadas automaticamente ao grupo de segurança.

> **Observação:**
>
> Para renomear o grupo de segurança do Microsoft Entra após a criação do catálogo, edite o catálogo e vá para **Grupo de Segurança do Microsoft Entra** na navegação à esquerda. Os nomes dos grupos de segurança do Microsoft Entra não devem conter os seguintes caracteres: `@ " \ / ; : # . * ? = < > | [ ] ( ) '`.

6. Na página **Credenciais de Domínio**, siga as orientações no artigo Criar Catálogos de Máquinas para concluir as configurações.
7. Na página **Resumo**, revise as configurações especificadas e clique em **Concluir**.

> **Dica:**

> Você pode visualizar o custo mensal estimado para as máquinas virtuais neste catálogo de máquinas com base no preço de tabela público do Azure. Se a conexão que hospeda o catálogo tiver a permissão `Microsoft.Consumption/pricesheets/read` no Azure, a estimativa será calculada usando o preço contratado da sua organização.

> Selecione a estimativa de custo para ver informações detalhadas. Para uma estimativa mais precisa, ajuste as configurações, como horas de funcionamento diárias, dias úteis por semana e opções de economia com base no seu uso.

Criar uma especificação de modelo do Azure

Você pode criar uma especificação de modelo do Azure no portal do Azure e usá-la no Studio e em comandos do PowerShell para criar ou atualizar um catálogo de máquinas MCS.

Para criar uma especificação de modelo do Azure para uma VM existente:

1. Vá para o portal do Azure. Selecione um grupo de recursos e, em seguida, selecione a VM e a interface de rede. No menu **...** na parte superior, clique em **Exportar modelo**.
2. Desmarque a caixa de seleção **Incluir parâmetros** se quiser criar uma especificação de modelo para provisionamento de catálogo. Verifique no arquivo JSON se as seções `parameters` e `variables` são:

   ```
   "parameters": {},

   "variables": {}
   ```

3. Clique em **Baixar** para salvar o modelo como arquivo JSON.
4. No portal do Azure, selecione **Especificações de modelo** e clique em **Importar modelo**.
5. Procure e importe o perfil da máquina (em JSON) salvo em seu computador.
6. Forneça o **Nome**, **Assinatura**, **Grupo de Recursos**, **Localização** e **Versão**. Clique em **Avançar: Editar Modelo**.
7. Crie **Revisar+Criar** e crie a especificação de modelo.
8. Na página **Especificações de Modelo**, verifique a especificação de modelo que você criou. Clique na especificação de modelo. No painel esquerdo, clique em **Versões**.

9. Você pode criar uma nova versão clicando em **Criar nova versão**. Especifique um novo número de versão, faça alterações na especificação de modelo atual e clique em **Revisar + Criar** para criar a nova versão da especificação de modelo.

Você pode obter informações sobre a especificação de modelo e a versão do modelo usando os seguintes comandos do PowerShell:

- Para obter informações sobre a especificação de modelo, execute:

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- Para obter informações sobre a versão da especificação de modelo, execute:

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

Usar uma especificação de modelo na criação ou atualização de um catálogo

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode:

- Use o Studio. Consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Studio.
- Use o PowerShell. Consulte Usar especificação de modelo na criação ou atualização de um catálogo usando o PowerShell

Exportar um perfil de máquina para um arquivo JSON

Você pode exportar o perfil de máquina usado por um catálogo para um arquivo JSON. Essa função permite personalizar o perfil e importá-lo para o Azure como uma especificação de Modelo ARM para provisionamento futuro.

1. Na página **Catálogos de Máquinas**, selecione um catálogo de máquinas para visualizar os detalhes no painel inferior.
2. Clique na guia **Propriedades do Modelo** para visualizar as propriedades do perfil da máquina e clique em **Exportar**.

3. Especifique um caminho em seu computador local para salvar o perfil da máquina como um arquivo JSON.

Importar um perfil de máquina como uma especificação de Modelo ARM no Azure

1. No portal do Azure, selecione **Especificações de modelo** e clique em **Importar Modelo**.
2. Procure e importe o perfil da máquina (em JSON) salvo em seu computador.
3. Forneça o **Nome**, **Assinatura**, **Grupo de Recursos**, **Local** e **Versão** para o modelo de importação e clique em **Revisar + Criar**. O modelo é validado e importado com sucesso. O modelo importado é listado em **Especificações de modelo**.

Ao criar catálogos de máquinas usando perfis de máquina, você pode ver este modelo ao escolher perfis. Para obter mais informações, consulte Usar uma especificação de modelo na criação ou atualização de um catálogo.

Provisionar máquinas em Zonas de Disponibilidade especificadas

Você pode provisionar máquinas em Zonas de Disponibilidade específicas em ambientes Azure. Você pode conseguir isso usando o Studio ou o PowerShell.

> **Nota:**
>
> - Se nenhuma zona for especificada, o MCS permite que o Azure coloque as máquinas dentro da região. Se mais de uma zona for especificada, o MCS distribui aleatoriamente as máquinas entre elas.
> - Se você selecionar ZRS como redundância de armazenamento na página Tipos de Armazenamento e Licença, receberá um aviso sugerindo que desmarque a seleção de zona e deixe o Azure gerenciar as zonas de disponibilidade da VM. Você receberá o aviso somente se selecionar um perfil de máquina ou grupo de host que tenha zonas de disponibilidade.

Configurar Zonas de Disponibilidade no Studio

Ao criar um catálogo de máquinas, você pode especificar as Zonas de Disponibilidade nas quais deseja provisionar máquinas. Na página **Máquinas Virtuais**, selecione uma ou mais Zonas de Disponibilidade onde deseja criar máquinas.

Há duas razões pelas quais nenhuma Zona de Disponibilidade está disponível: A região não possui Zonas de Disponibilidade ou o tamanho da máquina selecionada está indisponível.

Para obter informações sobre como configurar usando o comando PowerShell, consulte Configurar Zonas de Disponibilidade usando PowerShell.

Discos efêmeros do Azure

Um disco efêmero do Azure permite que você reutilize o disco de cache, disco temporário ou disco NVMe para armazenar o disco do SO para uma máquina virtual habilitada para Azure. Essa funcionalidade é útil para ambientes Azure que exigem um disco SSD de maior desempenho em vez de um disco HDD padrão. Para obter informações sobre como criar um catálogo com um disco efêmero do Azure, consulte Criar um catálogo com um disco efêmero do Azure.

> **Nota:**
>
> Catálogos persistentes não suportam discos de SO efêmeros.

> Discos de SO efêmeros exigem que seu esquema de provisionamento use discos gerenciados e uma Galeria de Computação do Azure. Para obter mais informações, consulte Galeria de imagens compartilhadas do Azure.

Armazenar um disco temporário de SO efêmero

Você tem a opção de armazenar um disco de SO efêmero no disco temporário da VM, em um disco de recurso ou em um disco NVMe. Essa funcionalidade permite que você use um disco de SO efêmero com uma VM que não possui cache ou possui cache insuficiente. Essas VMs possuem um disco temporário, disco de recurso ou disco NVMe para armazenar um disco de SO efêmero, como `Ddv4`.

Considere o seguinte:

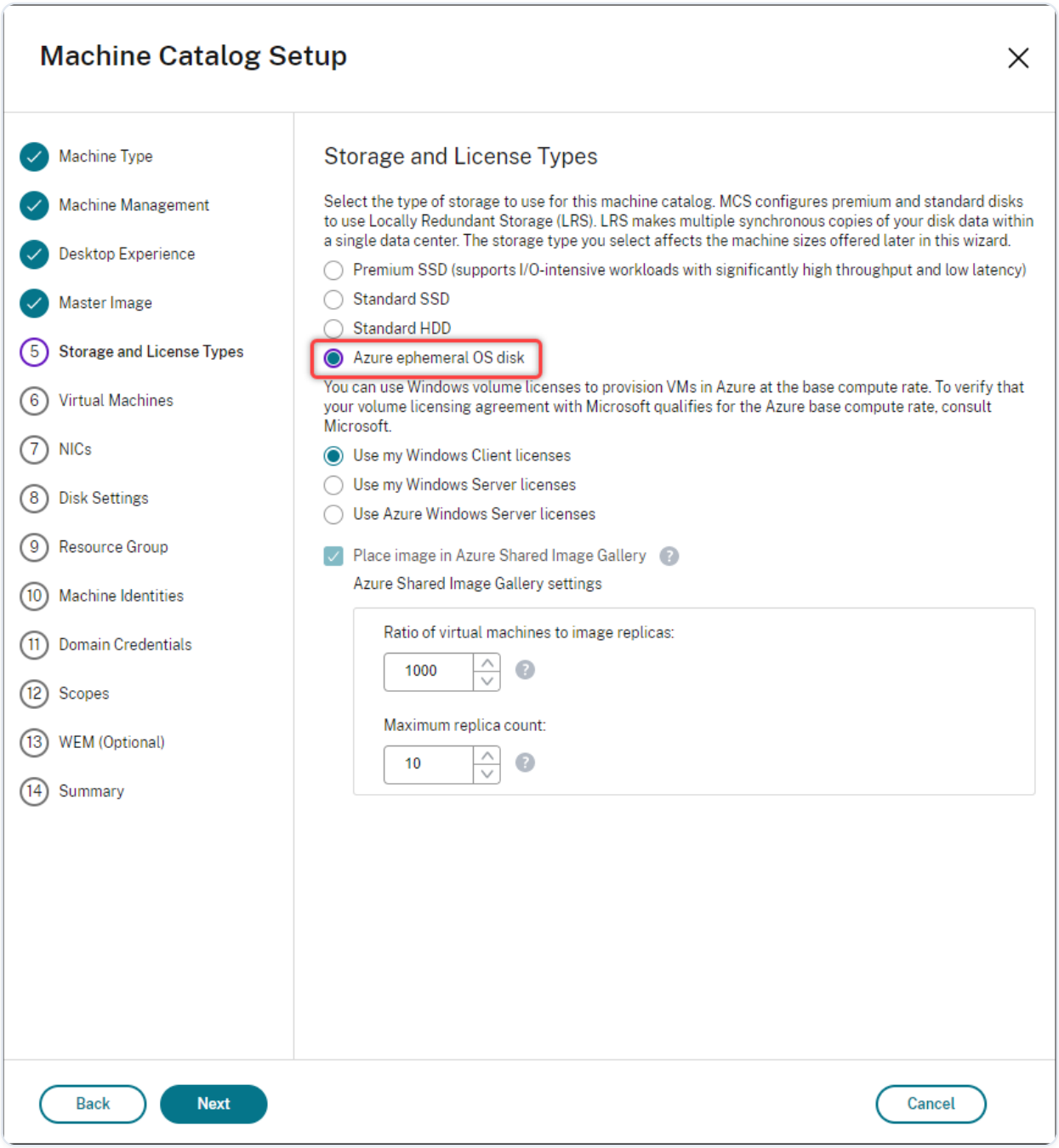
- Um disco efêmero é armazenado no disco de cache da VM, ou no disco temporário (de recurso) da VM ou no disco NVMe. O disco de cache é preferido em relação ao disco temporário, a menos que o disco de cache não seja grande o suficiente para conter o conteúdo do disco do SO.
- Para atualizações, uma nova imagem que é maior que o disco de cache, mas menor que o disco temporário, resulta na substituição do disco de SO efêmero pelo disco temporário da VM.

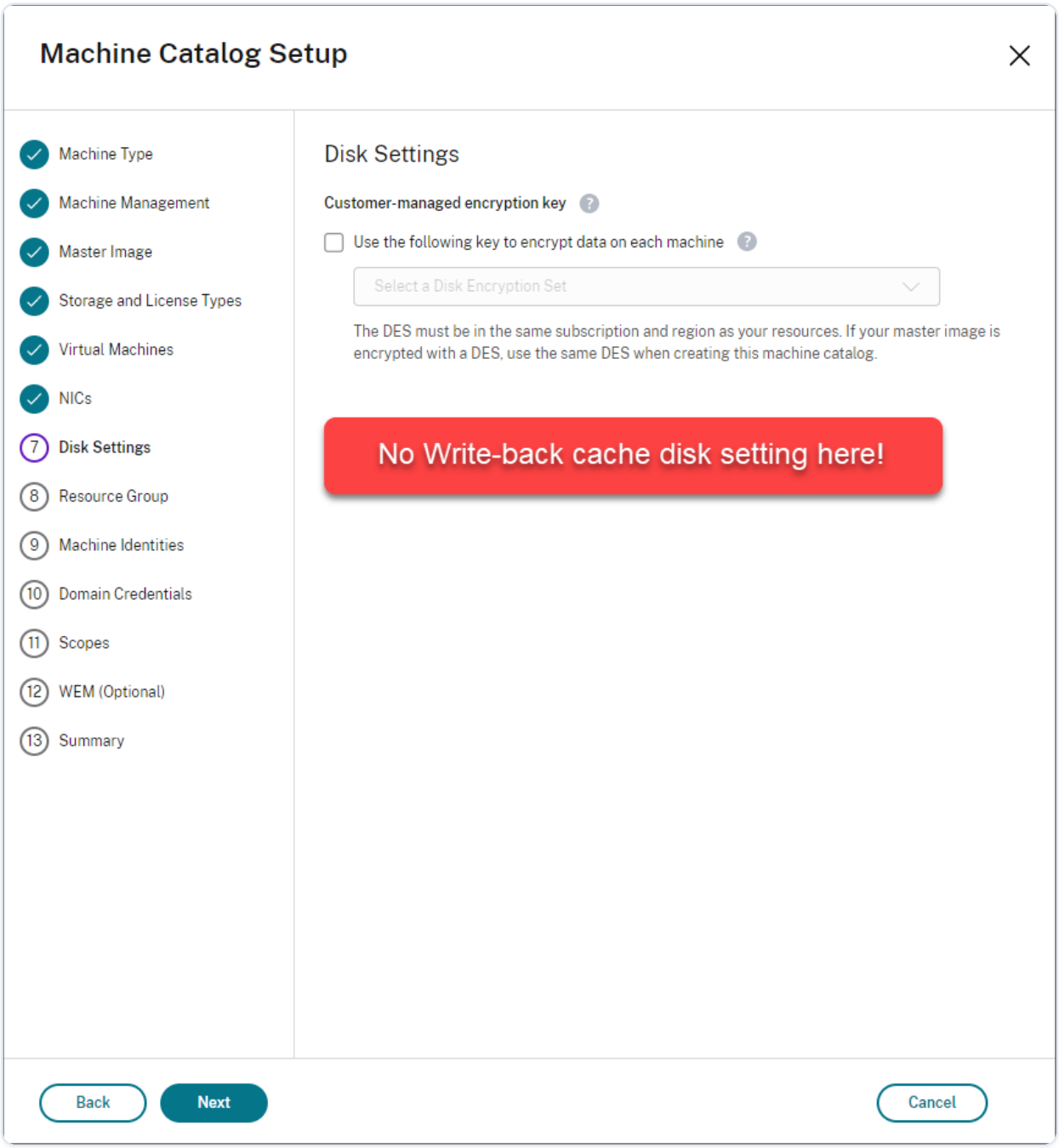
Disco efêmero do Azure e otimização de armazenamento do Machine Creation Services (MCS) (MCS I/O)

O disco de SO efêmero do Azure e o MCS I/O não podem ser ativados ao mesmo tempo.

As considerações importantes são as seguintes:

- Você não pode criar um catálogo de máquinas com o disco de SO efêmero e o MCS I/O ativados ao mesmo tempo.
- No assistente de **Configuração do Catálogo de Máquinas**, se você selecionar **Disco de SO efêmero do Azure** na página **Tipos de Armazenamento e Licença**, você não terá a opção de configurações de disco de cache de write-back na página **Configurações de Disco**.





- Os parâmetros do PowerShell (`UseWriteBackCache` e `UseEphemeralOsDisk`) definidos como **true** em `New-ProvScheme` ou `Set-ProvScheme` falham com uma mensagem de erro apropriada.
- Para catálogos de máquinas existentes criados com ambas as funcionalidades ativadas, você ainda pode:
  - atualizar um catálogo de máquinas.
  - adicionar ou excluir VMs.
  - excluir um catálogo de máquinas.

Galeria de Computação do Azure

Use a Galeria de Computação do Azure (anteriormente Galeria de Imagens Compartilhadas) como um repositório de imagens publicado para máquinas provisionadas por MCS no Azure. Você pode armazenar uma imagem publicada na galeria para acelerar a criação e a hidratação de discos de SO, melhorando os tempos de inicialização e de lançamento de aplicativos para VMs não persistentes. A Galeria de Computação do Azure contém os três elementos a seguir:

- Galeria: As imagens são armazenadas aqui. O MCS cria uma galeria para cada catálogo de máquinas.
- Definição de Imagem da Galeria: Esta definição inclui informações (tipo e estado do sistema operacional, região do Azure) sobre a imagem publicada. O MCS cria uma definição de imagem para cada imagem criada para o catálogo.
- Versão da Imagem da Galeria: Cada imagem em uma Galeria de Computação do Azure pode ter várias versões, e cada versão pode ter várias réplicas em diferentes regiões. Cada réplica é uma cópia completa da imagem publicada. O Citrix DaaS cria uma versão de imagem Standard_LRS (versão 1.0.0) para cada imagem com o número apropriado de réplicas na região do catálogo, com base no número de máquinas no catálogo, na taxa de réplica configurada e no máximo de réplicas configurado.

> **Nota:**
>
> A funcionalidade da Galeria de Computação do Azure é compatível apenas com discos gerenciados. Não está disponível para catálogos de máquinas legados.

> Para obter mais informações, consulte Visão geral da galeria de imagens compartilhadas do Azure.

Acessar imagens da Galeria de Computação do Azure

Ao selecionar uma imagem para usar na criação de um catálogo de máquinas, você pode selecionar imagens que criou na Galeria de Computação do Azure. Essas imagens aparecem na lista de imagens na página **Imagem** do assistente de Configuração do Catálogo de Máquinas.

Para que essas imagens apareçam, você deve:

1. Configurar o Citrix DaaS.
2. Conectar-se ao Azure Resource Manager.

3. No portal do Azure, crie um grupo de recursos. Para obter detalhes, consulte Criar uma Galeria de Imagens Compartilhadas do Azure usando o portal.
4. No grupo de recursos, crie uma Galeria de Computação do Azure.
5. Na Galeria de Computação do Azure, crie uma definição de imagem.
6. Na definição de imagem, crie uma versão de imagem.

Para obter informações sobre como configurar a Galeria de Computação do Azure, consulte Configurar a Galeria de Computação do Azure.

Condições para que o disco temporário do Azure seja elegível para disco de cache de write-back

Você pode usar o disco temporário do Azure como disco de cache de write-back somente se todas as seguintes condições forem satisfeitas:

- O disco de cache de write-back não deve ser persistente, pois o disco temporário do Azure não é apropriado para dados persistentes.
- O tamanho da VM do Azure escolhido deve incluir um disco temporário.
- O disco do SO efêmero não precisa ser habilitado.
- Aceitar colocar o arquivo de cache de write-back no disco temporário do Azure.
- O tamanho do disco temporário do Azure deve ser maior que o tamanho total de (tamanho do disco de cache de write-back + espaço reservado para arquivo de paginação + 1 GB de espaço de buffer).

Cenários de disco de cache de write-back não persistente

A tabela a seguir descreve três cenários diferentes em que um disco temporário é usado para cache de write-back ao criar um catálogo de máquinas.

CENÁRIO	RESULTADO
Todas as condições para usar um disco temporário para cache de write-back são satisfeitas.	O arquivo WBC `mcsdif.vhdx` é colocado no disco temporário.
O disco temporário tem espaço insuficiente para uso do cache de write-back.	Um disco VHD 'MCSWCDisk' é criado e o arquivo WBC `mcsdif.vhdx` é colocado neste disco.

CENÁRIO	RESULTADO
O disco temporário tem espaço suficiente para o uso do cache de write-back, mas `UseTempDiskForWBC` está definido como falso.	Um disco VHD 'MCSWCDisk' é criado e o arquivo WBC `mcsdif.vhdx` é colocado neste disco.

Consulte os seguintes tópicos do PowerShell:

- Criar um catálogo de máquinas com disco de cache de write-back não persistente
- Criar um catálogo de máquinas com disco de cache de write-back persistente

Criptografia do lado do servidor do Azure

O Citrix DaaS oferece suporte a chaves de criptografia gerenciadas pelo cliente para discos gerenciados do Azure por meio do Azure Key Vault. Com esse suporte, você pode gerenciar seus requisitos organizacionais e de conformidade criptografando os discos gerenciados do seu catálogo de máquinas usando sua própria chave de criptografia. Para obter mais informações, consulte Criptografia do lado do servidor do Armazenamento em Disco do Azure.

Ao usar esse recurso para discos gerenciados:

- Para alterar a chave com a qual o disco é criptografado, você altera a chave atual no `DiskEncryptionSet`. Todos os recursos associados a esse `DiskEncryptionSet` mudam para serem criptografados com a nova chave.
- Quando você desativa ou exclui sua chave, todas as VMs com discos que usam essa chave são desligadas automaticamente. Após o desligamento, as VMs não são utilizáveis, a menos que a chave seja ativada novamente ou você atribua uma nova chave. Qualquer catálogo que use a chave não pode ser ligado, e você não pode adicionar VMs a ele.

Considerações importantes ao usar chaves de criptografia gerenciadas pelo cliente

Considere o seguinte ao usar este recurso:

- Todos os recursos relacionados às suas chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem residir na mesma assinatura e região.
- Discos, instantâneos e imagens criptografados com chaves gerenciadas pelo cliente não podem ser movidos para outro grupo de recursos e assinatura.
- Consulte o site da Microsoft para obter informações sobre as limitações dos conjuntos de criptografia de disco por região.

Nota:

Consulte Início Rápido: Criar um Key Vault usando o portal do Azure para obter informações sobre como configurar a criptografia do lado do servidor do Azure.

Chave de criptografia gerenciada pelo cliente do Azure

Ao criar um catálogo de máquinas, você pode escolher se deseja criptografar os dados nas máquinas provisionadas no catálogo. A criptografia do lado do servidor com uma chave de criptografia gerenciada pelo cliente permite gerenciar a criptografia em um nível de disco gerenciado e proteger os dados nas máquinas do catálogo. Um Conjunto de Criptografia de Disco (DES) representa uma chave gerenciada pelo cliente. Para usar esse recurso, você deve primeiro criar seu DES no Azure. Um DES está no seguinte formato:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

Selecione um DES na lista. O DES selecionado deve estar na mesma assinatura e região que seus recursos.

Se você criar um catálogo com uma chave de criptografia e, posteriormente, desativar o DES correspondente no Azure, não poderá mais ligar as máquinas no catálogo ou adicionar máquinas a ele.

Consulte Criar um catálogo de máquinas com chave gerenciada pelo cliente.

Criptografia de disco do Azure no host

Você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host. Atualmente, o MCS oferece suporte apenas ao fluxo de trabalho de perfil de máquina para esse recurso. Você pode usar uma VM ou uma especificação de modelo como entrada para um perfil de máquina.

Esse método de criptografia não criptografa os dados por meio do armazenamento do Azure. O servidor que hospeda a VM criptografa os dados e, em seguida, os dados criptografados fluem pelo servidor de armazenamento do Azure. Portanto, esse método de criptografia criptografa os dados de ponta a ponta.

Restrições:

A criptografia de disco do Azure no host é:

- Não suportada para todos os tamanhos de máquina do Azure
- Incompatível com a criptografia de disco do Azure

Para obter mais informações, consulte:

- Criar um catálogo de máquinas com capacidade de criptografia no host.
- Recuperar informações de criptografia no host de um perfil de máquina

Criptografia dupla em disco gerenciado

Você pode criar um catálogo de máquinas com criptografia dupla. Quaisquer catálogos criados com esse recurso têm todos os discos criptografados no lado do servidor com chaves gerenciadas pela plataforma e pelo cliente. Você possui e mantém o Azure Key Vault, a Chave de Criptografia e os Conjuntos de Criptografia de Disco (DES).

A criptografia dupla é a criptografia do lado da plataforma (padrão) e a criptografia gerenciada pelo cliente (CMEK). Portanto, se você é um cliente altamente sensível à segurança que está preocupado com o risco associado a qualquer algoritmo de criptografia, implementação ou uma chave comprometida, você pode optar por essa criptografia dupla. Discos de SO e dados persistentes, instantâneos e imagens são todos criptografados em repouso com criptografia dupla.

> **Nota:**
>
> - Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Studio e comandos do PowerShell.
> - Você pode usar o fluxo de trabalho baseado em perfil não-máquina ou o fluxo de trabalho baseado em perfil de máquina para criar ou atualizar um catálogo de máquinas com criptografia dupla.
> - Se você usar o fluxo de trabalho baseado em perfil não-máquina para criar um catálogo de máquinas, poderá reutilizar o `DiskEncryptionSetId` armazenado.
> - Se você usar um perfil de máquina, poderá usar uma VM ou especificação de modelo como entrada de perfil de máquina.

Limitações

- A criptografia dupla não é suportada para Ultra Disks ou discos Premium SSD v2.
- A criptografia dupla não é suportada em discos não gerenciados.

- Se você desabilitar uma chave de Conjunto de Criptografia de Disco associada a um catálogo, as VMs do catálogo serão desabilitadas.
- Todos os recursos relacionados às suas chaves gerenciadas pelo cliente (Azure Key Vaults, conjuntos de criptografia de disco, VMs, discos e instantâneos) devem estar na mesma assinatura e região.
- Você pode criar apenas até 50 conjuntos de criptografia de disco por região por assinatura.

Consulte os seguintes tópicos do PowerShell:

- Criar um catálogo de máquinas com criptografia dupla
- Converter um catálogo não criptografado para usar criptografia dupla
- Verificar se o catálogo está com criptografia dupla

Grupos de recursos do Azure

Os grupos de recursos de provisionamento do Azure fornecem uma maneira de provisionar as VMs que fornecem aplicativos e desktops aos usuários. Você pode criar um grupo de recursos ou usar um grupo de recursos existente para provisionar VMs em um catálogo de máquinas MCS. Você pode usar o mesmo grupo de recursos em vários catálogos de máquinas. Para obter informações sobre grupos de recursos do Azure, consulte a documentação da Microsoft.

Uso do Grupo de Recursos do Azure

Não há limite para o número de máquinas virtuais, discos gerenciados, instantâneos e imagens por Grupo de Recursos do Azure. (O limite de 240 VMs por 800 discos gerenciados por Grupo de Recursos do Azure foi removido.)

- Ao usar um principal de serviço de escopo total para criar um catálogo de máquinas, o MCS cria apenas um Grupo de Recursos do Azure e usa esse grupo para o catálogo.
- Ao usar um principal de serviço de escopo restrito para criar um catálogo de máquinas, você deve fornecer um Grupo de Recursos do Azure vazio e pré-criado para o catálogo.

Azure Marketplace

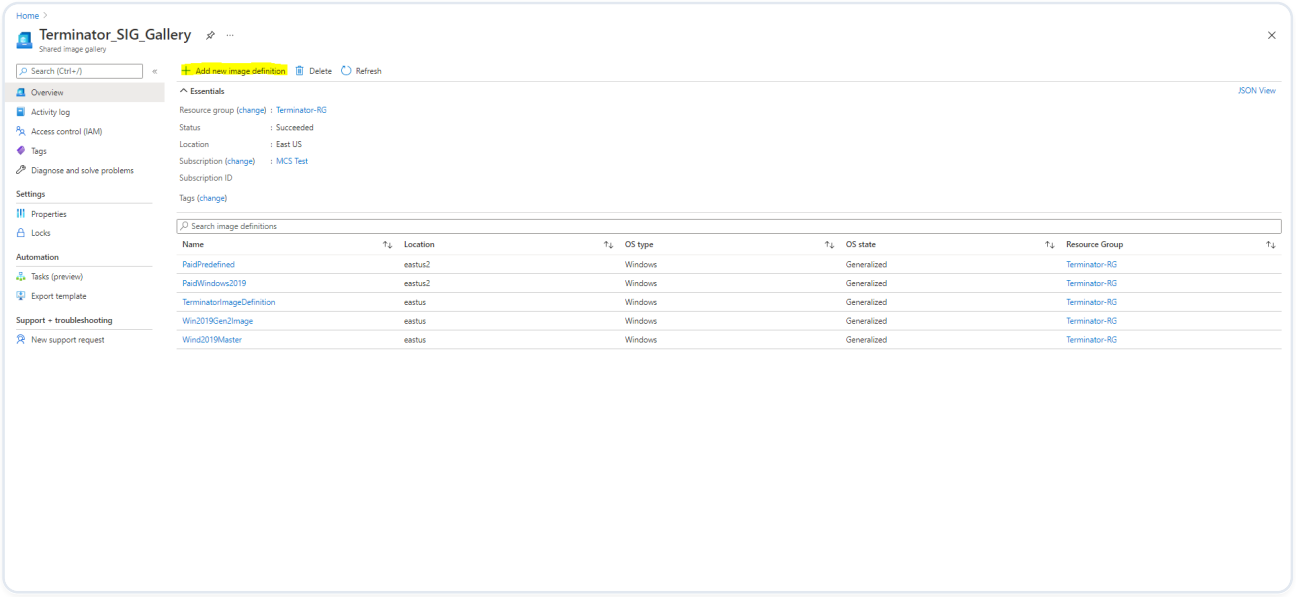
O Citrix DaaS oferece suporte ao uso de uma imagem mestre no Azure que contém informações de plano para criar um catálogo de máquinas. Para obter mais informações, consulte Microsoft Azure Marketplace.

> **Dica:**

> Algumas imagens encontradas no Azure Marketplace, como a imagem padrão do Windows Server, não anexam informações de plano. O recurso Citrix DaaS é para imagens pagas.

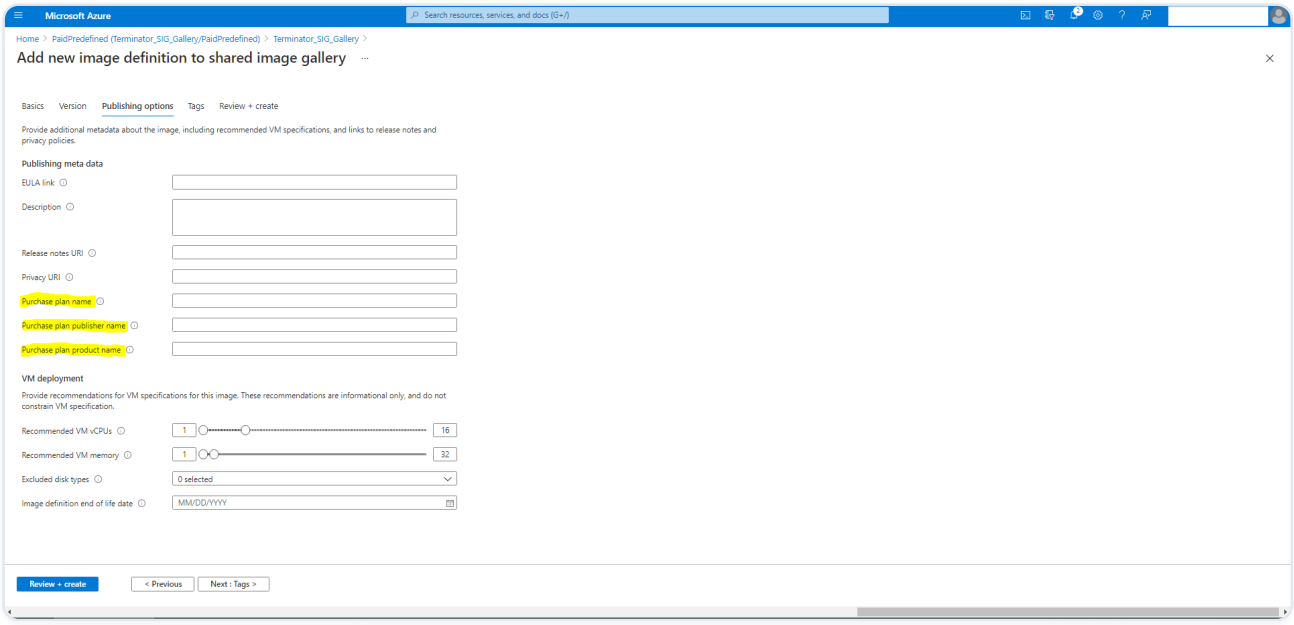
Certifique-se de que a imagem criada na Galeria de Computação do Azure contenha informações de plano do Azure

Use o procedimento nesta seção para visualizar imagens da Galeria de Computação do Azure no Studio. Essas imagens podem ser usadas opcionalmente para uma imagem mestre. Para colocar a imagem em uma Galeria de Computação do Azure, crie uma definição de imagem em uma galeria.

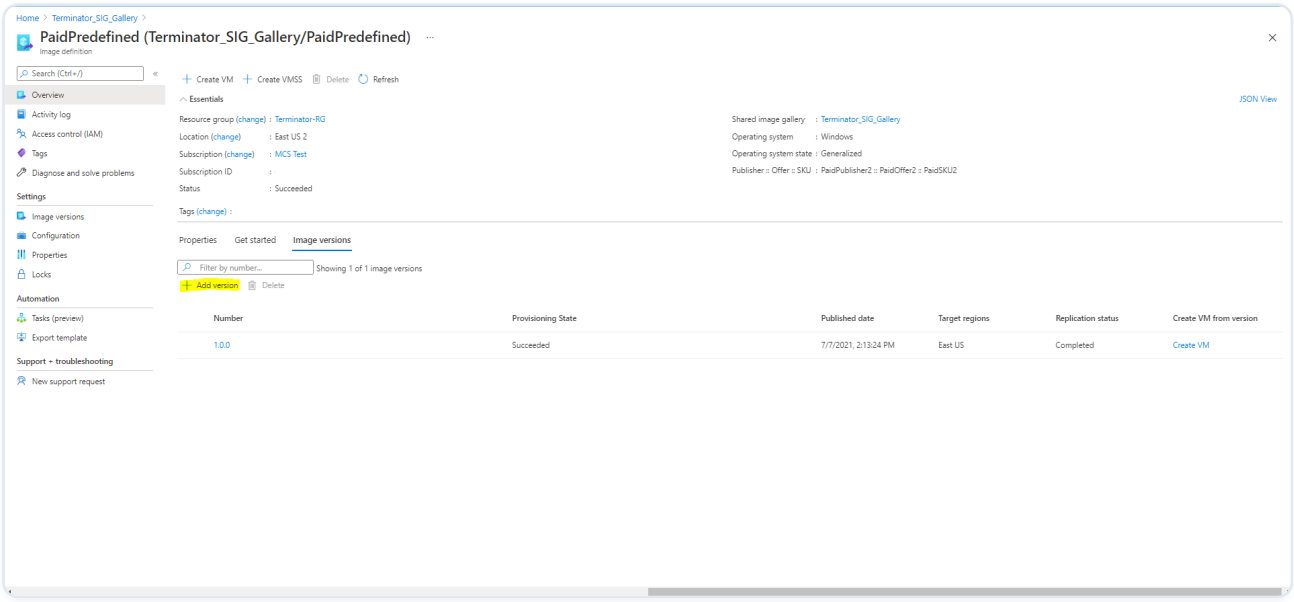


Na página **Opções de publicação**, verifique as informações do plano de compra.

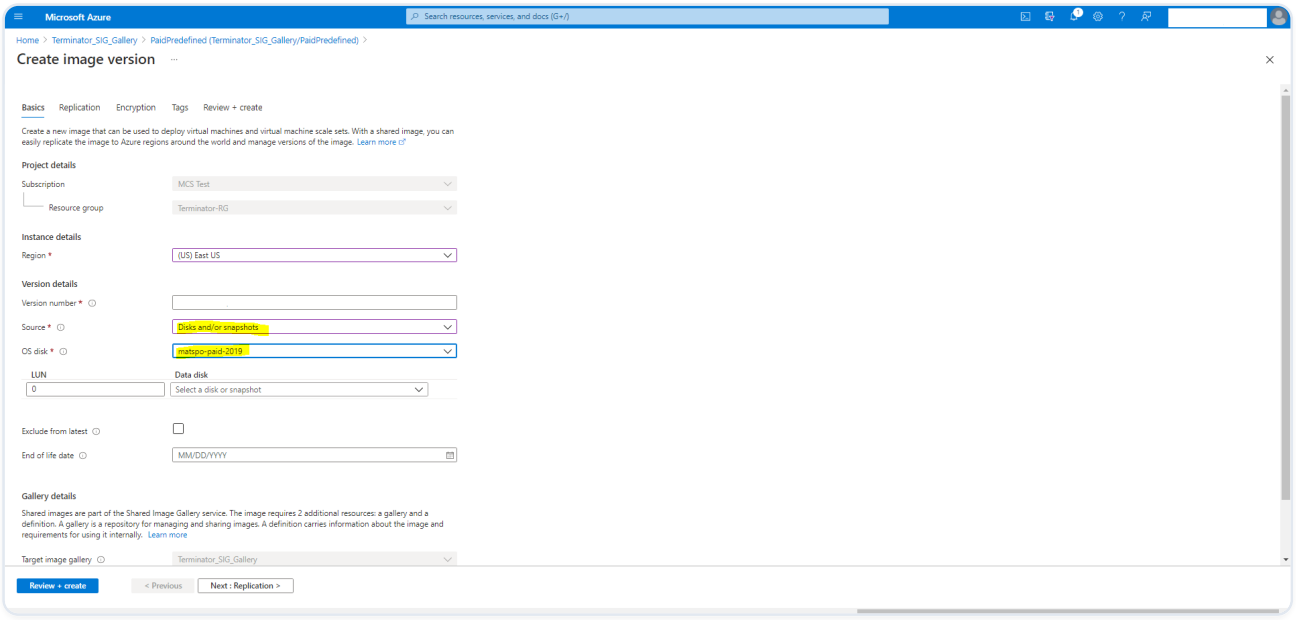
Os campos de informações do plano de compra estão inicialmente vazios. Preencha esses campos com as informações do plano de compra usadas para a imagem. A falha ao preencher as informações do plano de compra pode fazer com que o processo de catálogo de máquinas falhe.



Após verificar as informações do plano de compra, crie uma versão da imagem dentro da definição. Esta é usada como a imagem mestre. Clique em **Adicionar versão**:



Na seção **Detalhes da versão**, selecione o instantâneo da imagem ou o disco gerenciado como a origem:



Provisionar VMs de catálogo com o Agente do Azure Monitor instalado

O monitoramento do Azure é um serviço que você pode usar para coletar, analisar e agir sobre dados de telemetria de seus ambientes Azure e locais.

O Agente do Azure Monitor (AMA) coleta dados de monitoramento de recursos de computação como máquinas virtuais e entrega os dados ao monitor do Azure. Atualmente, ele suporta a coleta de Logs de Eventos, Syslog e métricas de Desempenho e os envia para as fontes de dados do Azure Monitor Metrics e Azure Monitor Logs.

Para habilitar o monitoramento identificando exclusivamente as VMs nos dados de monitoramento, você pode provisionar as VMs de um catálogo de máquinas MCS com o AMA instalado como uma extensão.

Requisitos

- Permissões: Certifique-se de ter as permissões mínimas do Azure conforme especificado em Sobre as permissões do Azure e as seguintes permissões para usar o Azure Monitor:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Regra de Coleta de Dados: Configure uma regra de coleta de dados no portal do Azure. Para obter informações sobre como configurar uma DCR, consulte Criar uma regra de coleta de

dados. Uma DCR é específica da plataforma (Windows ou Linux). Certifique-se de criar uma DCR de acordo com a plataforma necessária. O AMA usa Regras de Coleta de Dados (DCR) para gerenciar o mapeamento entre os recursos, como VMs, e fontes de dados, como Azure Monitor Metrics e Azure Monitor Logs.

- Espaço de Trabalho Padrão: Crie um espaço de trabalho no portal do Azure. Para obter informações sobre como criar um, consulte Criar um espaço de trabalho do Log Analytics. Ao coletar logs e dados, as informações são armazenadas em um espaço de trabalho. Ele possui um ID de espaço de trabalho e um ID de recurso exclusivos. O nome dele deve ser exclusivo para um determinado grupo de recursos. Depois de criar um espaço de trabalho, configure as fontes de dados e as soluções para armazenar seus dados nele.
- Extensão de monitoramento na lista de permissões: As extensões `AzureMonitorWindowsAgent` e `AzureMonitorLinuxAgent` são extensões definidas pela Citrix na lista de permissões. Para visualizar a lista de extensões na lista de permissões, use o comando PowerShell, `Get-ProvMetadataConfiguration`.
- Imagem Mestra: A Microsoft recomenda remover extensões de uma máquina existente antes de criar uma nova máquina a partir dela. Se as extensões não forem removidas, isso pode levar a arquivos residuais e comportamento inesperado. Para obter mais informações, consulte Se a VM for recriada a partir de uma VM existente.

Para obter informações sobre como criar um catálogo com AMA habilitado usando o PowerShell, consulte Provisionar VMs de catálogo com AMA habilitado.

VMs confidenciais do Azure

As VMs de computação confidencial do Azure garantem que seu desktop virtual seja criptografado na memória e protegido em uso.

Você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho de perfil de máquina para criar tal catálogo. Você pode usar tanto VM quanto a especificação de modelo ARM como entrada de perfil de máquina.

Você também pode usar uma imagem mestre do Azure do tipo VM confidencial e um perfil de máquina do Azure do tipo VM confidencial para criar uma imagem preparada e, em seguida, usar esta imagem preparada para criar um catálogo MCS.

Considerações importantes para VMs confidenciais

As considerações importantes para tamanhos de VM suportados e criação de catálogo de máquinas com VMs confidenciais são as seguintes:

- Para verificar os tamanhos de VM suportados por VMs Confidenciais, consulte Tamanhos.
- Crie catálogos de máquinas com VMs confidenciais.
  - Você pode criar um catálogo de máquinas com VMs Confidenciais do Azure usando comandos do Studio e do PowerShell.
  - Você deve usar o fluxo de trabalho baseado em perfil de máquina para criar um catálogo de máquinas com VMs Confidenciais do Azure. Você pode usar uma VM ou especificação de modelo como entrada de perfil de máquina.
  - A imagem mestre e a entrada do perfil da máquina devem estar ambas habilitadas com o mesmo tipo de segurança confidencial. Diferentes recursos do Azure usam rótulos diferentes para indicar o tipo de VM confidencial.

    Para snapshot do Azure, disco gerenciado ou máquina virtual, os tipos de segurança são:

    - ConfidentialVM_DiskEncryptedWithCustomerKey.
    - ConfidentialVM_DiskEncryptedWithPlatformKey.
    - ConfidentialVM_VMGuestStateOnlyEncryptedWithPlatformKey

    Para a versão da especificação de modelo ARM do Azure, os tipos de segurança são:

    - VMGuestStateOnly: VM confidencial com apenas o estado do convidado da VM criptografado
    - DiskWithVMGuestState: VM confidencial com disco do SO e estado do convidado da VM criptografados com chave gerenciada pela plataforma ou chave gerenciada pelo cliente. Tanto o disco do SO normal quanto o efêmero podem ser criptografados.
  - Você pode obter informações de VM confidenciais de vários tipos de recursos, como disco gerenciado, instantâneo, imagem da Galeria de Computação do Azure, VM e especificação de modelo ARM, usando o parâmetro AdditionalData. Por exemplo:

    ```
    PS C:\Users\username> (get-item XDHyp:
    \HostingUnits\mynetwork\image.folder\username-dev-testing-
    rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
    ```

    Os campos de dados adicionais são:
  - DiskSecurityType
  - ConfidentialVMDiskEncryptionSetId
  - DiskSecurityProfiles

Para obter a propriedade de computação confidencial de um tamanho de máquina, execute o seguinte comando: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

O campo de dados adicionais é `ConfidentialComputingType`.

- Você não pode alterar a imagem mestre ou o perfil da máquina de tipo de segurança confidencial para não confidencial, ou de não confidencial para confidencial.
- Você recebe mensagens de erro apropriadas para qualquer configuração incorreta.

Preparar imagens mestre e perfis de máquina

Antes de criar um conjunto de VMs confidenciais, siga estas etapas para preparar uma imagem mestre e um perfil de máquina para elas:

1. No portal do Azure, crie uma VM confidencial com configurações específicas, como:
   - **Tipo de Segurança**: Máquinas virtuais confidenciais
   - **Criptografia de disco do SO confidencial**: Habilitado.
   - **Gerenciamento de chaves**: Criptografia de disco confidencial com uma chave gerenciada pela plataforma Para obter mais informações sobre como criar VMs confidenciais, consulte este artigo da Microsoft.
2. Prepare a imagem mestre na VM criada. Instale os aplicativos necessários e o VDA na VM criada.

   > **Nota:**
   >
   > A criação de VMs confidenciais usando VHD não é suportada. Em vez disso, use a Galeria de Computação do Azure, discos gerenciados ou instantâneos para essa finalidade.

3. Crie o perfil da máquina usando uma destas formas:
   - Use a VM existente criada na etapa 1 se ela possuir as propriedades de máquina necessárias.
   - Se você optar por uma especificação de modelo ARM como perfil da máquina, crie a especificação de modelo conforme necessário. Especificamente, configure parâmetros que atendam aos seus requisitos de VM confidencial, como *SecurityEncryptionType* e

diskEncryptionSet (para chave gerenciada pelo cliente). Para obter mais informações, consulte Criar uma especificação de modelo do Azure.

> **Nota:**
>
> - Certifique-se de que a imagem mestre e o perfil da máquina tenham o mesmo tipo de chave de segurança.
> - Para criar VMs confidenciais que exigem criptografia de disco do SO confidencial com uma chave gerenciada pelo cliente, certifique-se de que os IDs do conjunto de criptografia de disco na imagem mestre e no perfil da máquina sejam idênticos.

Se você deseja usar uma imagem preparada do tipo VM confidencial para criar um catálogo MCS, crie uma imagem preparada usando a imagem mestre do tipo VM confidencial e um perfil de máquina do tipo VM confidencial. Consulte Criar uma definição de imagem e versão inicial da imagem para obter informações sobre como criar imagens preparadas.

Criar VMs confidenciais usando comandos do Studio ou PowerShell

Para criar um conjunto de VMs confidenciais, crie um catálogo de máquinas usando uma imagem mestre e um perfil de máquina derivado de uma VM confidencial desejada.

Para criar o catálogo usando o Studio, siga as etapas descritas em Criar catálogos de máquinas. Tenha as seguintes considerações em mente:

- Na página **Imagem**, selecione uma imagem mestre e um perfil de máquina que você preparou para a criação da VM confidencial. A seleção do perfil da máquina é obrigatória e apenas perfis que correspondem ao mesmo tipo de criptografia de segurança da imagem mestre selecionada estão disponíveis para seleção.
- Na página **Máquinas Virtuais**, apenas os tamanhos de máquina que suportam VMs confidenciais aparecem para seleção.
- Na página **Configurações de Disco**, você não pode especificar o conjunto de criptografia de disco porque ele é herdado do perfil de máquina selecionado.

Monitoramento de Integridade de Inicialização

Se sua VM tiver Inicialização Segura e Módulo de Plataforma Confiável virtual (vTPM) habilitados, e a extensão GuestAttestation instalada, o Microsoft Defender for Cloud pode validar remotamente

que sua VM inicializa de forma saudável. Este monitoramento é chamado de Monitoramento de Integridade de Inicialização. Para mais informações sobre Monitoramento de Integridade de Inicialização, consulte Visão geral do monitoramento de integridade de inicialização.

Você pode habilitar o Monitoramento de Integridade de Inicialização para VMs de catálogo de máquinas MCS (VMs persistentes e não persistentes) usando um perfil de máquina (VM ou especificação de modelo). O Monitoramento de Integridade de Inicialização é suportado apenas para Inicialização Confiável e VMs Confidenciais.

Você pode atualizar um catálogo existente para usar a integridade de inicialização usando `Set-ProvScheme para apontar para um perfil de máquina com integridade de inicialização habilitada. Novas VMs adicionadas ao catálogo são então habilitadas com monitoramento de integridade.

Você também pode atualizar uma VM existente em um catálogo usando `Set-ProvVmUpdateTimeWindow`, `Set-ProvVm` ou Ciclos de Manutenção.

Você pode converter um(a):

- VM sem monitoramento de integridade para ter monitoramento de integridade.
- VM com monitoramento de integridade para sem monitoramento de integridade.

Criar catálogo de máquinas habilitado com monitoramento de integridade

Certifique-se de ter as seguintes permissões:

- `Microsoft.Compute/virtualMachines/extensions/read`
- `Microsoft.Compute/virtualMachines/extensions/write`

Faça o seguinte para criar um catálogo de máquinas MCS habilitado com monitoramento de integridade:

1. Crie um perfil de máquina (VM ou especificação de modelo) com a extensão `GuestAttestation`.
2. Crie um catálogo de máquinas MCS usando a entrada do perfil de máquina por meio da interface de configuração completa ou de comandos PowerShell.

> **Nota:**

> Você pode verificar o status `GuestAttestationExtensionEnabled` de uma VM ou especificação de modelo usando o comando PowerShell `Get-Item` com `AdditionalData parameter`.

3. Adicione VMs ao catálogo.

Crie um perfil de máquina habilitado com a extensão GuestAttestation

Crie uma VM ou especificação de modelo como entrada de perfil de máquina com monitoramento de integridade habilitado, o que implica que a extensão `GuestAttestation` está instalada.

Para criar uma VM com monitoramento de integridade habilitado, faça o seguinte:

1. Entre no portal do Azure.
2. Se você estiver criando uma nova VM:
   a. Selecione **Tipo de segurança** como **Máquinas virtuais de inicialização confiável** ou **Máquinas virtuais confidenciais**.
   b. Clique em **Configurar recursos de segurança** e selecione a caixa de seleção **Monitoramento de integridade**.

> **Nota:**
>
> Para o monitoramento de integridade, você deve habilitar o Secure Boot e o vTPM.

3. Na página **Visão geral**, vá para a seção **Tipo de segurança** e verifique se o Tipo de segurança é Inicialização Confiável ou Máquinas virtuais confidenciais e se o Monitoramento de integridade está habilitado.
4. navegar para a página **Extensões + aplicativos** para verificar se `GuestAttestation` está instalado.

Para habilitar o monitoramento de integridade de uma VM existente, consulte Habilitar monitoramento de integridade - portal do Azure.

Para criar uma especificação de modelo com a extensão `GuestAttestation` instalada:

1. Você pode instalar o GuestAttestation usando uma especificação de modelo. Consulte Habilitar monitoramento de integridade - especificação de modelo.

> **Nota:**
>
> Nesta especificação de modelo, em **Configurações**, você pode configurar os pontos de extremidade a serem usados para atestado. Se você não configurar, o Azure decidirá quais pontos de extremidade configurar.

Criar um catálogo de VMs de reserva de capacidade sob demanda

A reserva de capacidade sob demanda permite reservar capacidade de computação em uma região do Azure ou Zona de Disponibilidade por qualquer período de tempo. Para obter mais informações sobre a reserva de capacidade sob demanda do Azure, consulte a documentação da Microsoft Reserva de Capacidade sob Demanda.

Você pode criar um catálogo de máquinas MCS de VMs do Azure com reserva de capacidade sob demanda usando um perfil de máquina (VM ou especificação de modelo). Você também pode atualizar um catálogo de máquinas existente e VMs existentes para ter ou remover a reserva de capacidade sob demanda.

Este recurso é aplicável a catálogos de máquinas persistentes e não persistentes.

Limitações

Este recurso não é aplicável a:

- VMs Spot
- Grupo de host
- VMs com hibernação ativada

Para mais informações sobre limitações, consulte a documentação da Microsoft Limitações e restrições.

Permissão necessária

Você precisa da seguinte permissão para criar um catálogo de VMs de reserva de capacidade sob demanda:

`Microsoft.Compute/capacityReservationGroups/deploy/action`

Etapas para criar um catálogo de VMs de reserva de capacidade sob demanda

1. Crie uma fonte de perfil de máquina (VM ou especificação de modelo ARM). Para criar uma VM ou uma especificação de modelo ARM, consulte Associar uma VM a um grupo de reserva de capacidade.
2. Execute o seguinte comando PowerShell para verificar se um perfil de máquina tem a reserva de capacidade sob demanda ativada ou não. Se o perfil de máquina estiver ativado com reserva de capacidade sob demanda, você obterá o `capacityReservationGroup id`.

   Por exemplo,

   Se a fonte do perfil da máquina for uma VM, execute o seguinte comando:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\demand-
   capacity.vm").AdditionalData
   ```

   Se a fonte do perfil da máquina for uma especificação de modelo, execute o seguinte comando:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
   templatespec.templatespec\14.0.0-capacity-
   reservation.templatespecversion").AdditionalData
   ```

3. Crie um catálogo de máquinas usando um perfil de máquina com comandos do Studio ou PowerShell.

Você pode atualizar um catálogo usando o comando `Set-ProvScheme`. Você também pode atualizar VMs existentes usando o comando PowerShell `Set-ProvVmUpdateTimeWindow`. O perfil da máquina é atualizado no próximo ligar.

Virtualização aninhada

Se você configurar a VM mestre com a virtualização aninhada ativada, todas as VMs no catálogo de máquinas MCS criadas usando essa VM mestre terão a virtualização aninhada ativada. Este recurso é aplicável a VMs persistentes e não persistentes. Você pode atualizar um catálogo de máquinas MCS existente e VMs existentes para ter virtualização aninhada por meio da atualização de imagem.

Atualmente, apenas os tamanhos de VM Dv3 e Ev3 suportam virtualização aninhada.

Para obter informações sobre virtualização aninhada, consulte o blog da Microsoft Virtualização Aninhada no Azure.

SKUs somente NVMe

Normalmente, as gerações mais antigas de VMs de uso geral, otimizadas para memória e otimizadas para computação (D/Ev5 ou Fv2 e anteriores) suportam SCSI. As gerações mais recentes (Da/Ea/Fav6 e posteriores) normalmente suportam apenas a interface de armazenamento NVMe. O MCS suporta o tipo de controlador de armazenamento NVMe para suportar os novos SKUs de VM no Azure.

Para obter informações sobre NVMe, consulte a documentação da Microsoft Perguntas Frequentes Gerais sobre NVMe.

Você pode criar um catálogo MCS usando uma oferta de serviço que:

- suporta SCSI e NVMe, consulte Criar um catálogo usando uma oferta de serviço que suporta SCSI e NVMe
- suporta apenas NVMe, consulte Criar um catálogo usando uma oferta de serviço que suporta apenas NVMe

Limitações

- Todas as ofertas de serviço que suportam NVMe não suportam o Trusted Launch ao mesmo tempo.
- NVMe não é suportado para VMs Gen 1.
- Algumas imagens de SO podem não suportar NVMe. Nesse caso, a opção NVMe fica esmaecida na interface do usuário do Azure.

Criar um catálogo usando uma oferta de serviço que suporta SCSI e NVMe

1. Crie uma VM para ser usada como imagem mestre.

    a. Use uma imagem do marketplace que suporte NVMe. Uma lista de imagens do Azure Marketplace que suportam NVMe pode ser encontrada em Imagens de SO suportadas para NVMe remoto.

    b. Tire um instantâneo do Disco do SO da VM para usar no parâmetro `MasterImageVM` do comando `New-ProvScheme` ou use o disco gerenciado diretamente.

    Verifique se sua imagem mestre suporta NVMe ou não usando uma das seguintes maneiras:

- Verifique o `SupportedDiskControllerTypes` no campo `AdditionalData` de `Get-Item`. Por exemplo:

  ```
  (get-item XDHyp:
  \HostingUnits\mynetwork\image.folder\abc.resourcegroup\deg-
  snapshot).AdditionalData
  ```

  O `SupportedDiskControllerTypes` deve ser `SCSI, NVMe`.

- Use o Azure CLI e o PowerShell

2. Use uma oferta de serviço que suporte NVMe e SCSI.
3. Use uma VM ou especificação de modelo como um perfil de máquina que tenha NVMe habilitado. Pegue qualquer VM que tenha `DiskControllerType` definido como NVMe. Use a VM diretamente como um perfil de máquina ou exporte o modelo e use a especificação do modelo como um perfil de máquina.

Crie um catálogo usando uma oferta de serviço que suporte apenas NVMe

1. Crie uma VM para ser usada como imagem mestre. Use uma imagem do marketplace que suporte NVMe. Uma lista de imagens do Azure Marketplace que suportam NVMe pode ser encontrada em Imagens de SO suportadas para NVMe remoto.
2. Use uma oferta de serviço que suporte apenas NVMe.

> **Nota:**
>
> Como a oferta de serviço suporta NVMe, você não precisa de um perfil de máquina com `DiskControllerType` definido como `NVMe` para habilitar o NVMe no catálogo. No entanto, se você usar um perfil de máquina, ele deve ter o `DiskControllerType` definido como `NVMe` ou deve estar em branco ou não especificado.

Modificar VMs persistentes existentes

A configuração NVMe não pode ser alterada em uma VM depois de criada. A maneira de alterar a configuração NVMe para uma VM persistente é reimplantar a VM. A lógica para fazer isso é:

1. Salve o estado atual da VM.
2. Após ligar uma VM existente, detecte se a VM requer reimplementação.

a. Se a alteração de configuração for de NVMe para NVMe ou de SCSI para SCSI, a reimplantação da VM não é necessária.

b. Se a alteração de configuração for de SCSI para NVMe e vice-versa, reimplemente e recrie a VM.

Usar PowerShell

Esta seção detalha como realizar as seguintes tarefas usando o PowerShell:

- Usar especificação de modelo na criação ou atualização de um catálogo usando PowerShell
- Habilitar extensões de VM do Azure
- Catálogos de máquinas com Inicialização Confiável
- Usar valores de propriedade de perfil de máquina
- Configurar Zonas de Disponibilidade usando PowerShell
- Provisionar VMs em hosts dedicados do Azure
- Configurar tipos de armazenamento
- Habilitar armazenamento com redundância de zona
- Capturar configurações de diagnóstico em VMs e NICs de um perfil de máquina
- Verificar a licença do Windows
- Configurar a licença do Linux
- Criar um catálogo de máquinas com um disco efêmero do Azure(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-with-an-azure-ephemeral-disk)
- Configurar a Galeria de Computação do Azure(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#configure-azure-compute-gallery)
- Criar ou atualizar um catálogo com várias NICs por VM(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-or-update-a-catalog-with-multiple-nics-per-vm)
- Criar um catálogo de máquinas com disco de cache de write-back não persistente(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-with-non-persistent-write-back-cache-disk)
- Criar um catálogo de máquinas com disco de cache de write-back persistente(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-with-persistent-write-back-cache-disk)

- Melhorar o desempenho de inicialização com MCSIO(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#improve-boot-performance-with-mcsio)
- Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-with-customer-managed-encryption-key)
- Criar um catálogo de máquinas com capacidade de criptografia no host(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-with-encryption-at-host-capability)
- Criar um catálogo de máquinas com criptografia dupla(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-with-double-encryption)
- Determinação do local do arquivo de paginação(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#page-file-location-determination)
- Cenários de configuração do arquivo de paginação(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#page-file-setting-scenarios)
- Especificar a configuração do arquivo de paginação(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#specify-page-file-setting)
- Modificar as configurações do arquivo de paginação(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#modify-page-file-settings)
- Provisionar VMs de catálogo com AMA habilitado(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#provision-catalog-vms-with-ama-enabled)
- Criar um catálogo usando VMs Spot do Azure(/pt-br/citrix-daas/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-catalog-using-azure-spot-vms)
- Configurar tamanhos de VM de backup
- Copiar tags em todos os recursos

Usar especificação de modelo na criação ou atualização de um catálogo usando PowerShell

Você pode criar ou atualizar um catálogo de máquinas MCS usando uma especificação de modelo como entrada de perfil de máquina. Para fazer isso, você pode usar o Studio ou comandos do PowerShell.

Para a interface do Studio, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager na interface do Studio.

Usando comandos do PowerShell:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*`.
3. Crie ou atualize um catálogo.

    - Para criar um catálogo:

        a. Use o comando `New-ProvScheme` com uma especificação de modelo como entrada de perfil de máquina. Por exemplo:

        ```
        New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
        image.folder/fgthj.resourcegroup/nab-ws-
        vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

        MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
        fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

        -ProvisioningSchemeName <String>

        -HostingUnitName <String>

        -IdentityPoolName <String>

        [-ServiceOffering <String>][-CustomProperties <String>]

        [<CommonParameters>]
        ```

        b. Conclua a criação do catálogo.

    - Para atualizar um catálogo, use o comando `Set-ProvScheme` com uma especificação de modelo como entrada de perfil de máquina. Por exemplo:

    ```
    Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
    Us.region/vm.folder/MasterDisk.vm'

    MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
    fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'
    ```

```
[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[<CommonParameters>]
```

Habilitar extensões de VM do Azure

Depois de selecionar a especificação de modelo ARM, execute os seguintes comandos do PowerShell para trabalhar com extensões de VM do Azure:

- Para visualizar a lista de extensões de VM do Azure suportadas: `Get-ProvMetadataConfiguration`
- Para adicionar mais extensões de VM: `Add-ProvMetadataConfiguration`. Por exemplo, `Add-ProvMetadataConfiguration -PluginType "AzureRM" -ConfigurationName "Extension" -ConfigurationValue "CustomScriptExtension"`

  Se você tentar adicionar qualquer um dos seguintes, o comando falhará com uma mensagem de erro:

  - Extensão definida pela Citrix.
  - Extensão definida pelo usuário existente.
  - Chaves de configuração não suportadas. Atualmente, a chave de configuração suportada é `Extension`.
- Para remover extensões da lista: `Remove-ProvMetadataConfiguration`. Você pode remover as extensões que adicionou.

Catálogos de máquinas com Inicialização Confiável

Para criar com sucesso um catálogo de máquinas com Inicialização Confiável, use:

- Uma imagem mestre habilitada com Inicialização Confiável. Você deve usar um perfil de máquina, no entanto, não é necessário que o perfil de máquina esteja habilitado para Inicialização Confiável. Se você usar uma imagem mestre habilitada com Inicialização Confiável e um perfil de máquina não habilitado para Inicialização Confiável, você receberá uma mensagem de aviso devido à configuração de Inicialização Confiável incompatível entre a imagem mestre e o perfil de máquina.
- Um tamanho de VM que suporta Inicialização Confiável.

- Uma versão de VM do Windows que suporta Inicialização Confiável. Atualmente, Windows 10, Windows 11, Windows Server 2016, 2019 e 2022 suportam Inicialização Confiável.

Para visualizar os itens de inventário da oferta do Citrix DaaS e determinar se o tamanho da VM suporta Inicialização Confiável, execute o seguinte comando:

1. Abra uma janela do PowerShell.
2. Execute **asnp citrix*** para carregar os módulos PowerShell específicos da Citrix.
3. Execute o seguinte comando:

   ```
   $s = (ls XDHyp:\HostingUnits\<name of hosting unit>\serviceoffering.folder\"<VM size>".serviceoffering)
   ```

4. Execute `$s | select -ExpandProperty Additionaldata`
5. Verifique o valor do atributo `SupportsTrustedLaunch`.

   - Se `SupportsTrustedLaunch` for **True**, o tamanho da VM oferece suporte ao Trusted Launch.
   - Se `SupportsTrustedLaunch` for **False**, o tamanho da VM não oferece suporte ao Trusted Launch.

De acordo com o PowerShell do Azure, você pode usar o seguinte comando para determinar os tamanhos de VM que oferecem suporte ao Trusted Launch:

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and ($_.Name -eq "<VM size>") })[0].Capabilities
```

A seguir estão exemplos que descrevem se o tamanho da VM oferece suporte ao Trusted Launch depois de executar o comando do Azure PowerShell.

- *Exemplo 1*: Se a VM do Azure suporta apenas a Geração 1, essa VM não suporta o Trusted Launch. Portanto, a capacidade `TrustedLaunchDisabled` não é exibida após a execução do comando do Azure PowerShell.
- *Exemplo 2*: Se a VM do Azure suporta apenas a Geração 2 e a capacidade `TrustedLaunchDisabled` for **True**, o tamanho da VM da Geração 2 não é suportado para o Trusted Launch.

- *Exemplo 3*: Se a VM do Azure suporta apenas a Geração 2 e a capacidade `TrustedLaunchDisabled` não for exibida após a execução do comando do PowerShell, o tamanho da VM da Geração 2 é suportado para o Trusted Launch.

Para obter mais informações sobre o Trusted Launch para máquinas virtuais do Azure, consulte o documento da Microsoft Trusted launch for Azure virtual machines.

Criar um catálogo de máquinas com Trusted Launch

1. Crie uma imagem mestre habilitada com Trusted Launch. Consulte a documentação da Microsoft Trusted launch VM Images.
2. Crie uma VM ou especificação de modelo com o tipo de segurança como **máquinas virtuais de inicialização confiável**. Para obter mais informações sobre como criar uma VM ou especificação de modelo, consulte o documento da Microsoft Deploy a trusted launch VM.
3. Crie um catálogo de máquinas usando o Studio ou comandos do PowerShell.

   - Se você quiser usar o Studio, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager no Studio.
   - Se você quiser usar comandos do PowerShell, use o comando `New-ProvScheme` com a VM ou a especificação de modelo como entrada de perfil de máquina.

     Exemplo de `New-ProvScheme` com VM como entrada de perfil de máquina:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name"
     -IdentityPoolName "name" -InitialBatchSizeHint 1

     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
     fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

     -MachineProfile "XDHyp:
     \HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
     hine profile vm.vm>"

     -ProvisioningSchemeName <String>

     -HostingUnitName <String>

     -IdentityPoolName <String>

     [-ServiceOffering <String>][-CustomProperties <String>]
     ```

```
[<CommonParameters>]
```

Exemplo de `New-ProvScheme` com especificação de modelo como entrada de perfil de máquina:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name"
-IdentityPoolName "name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

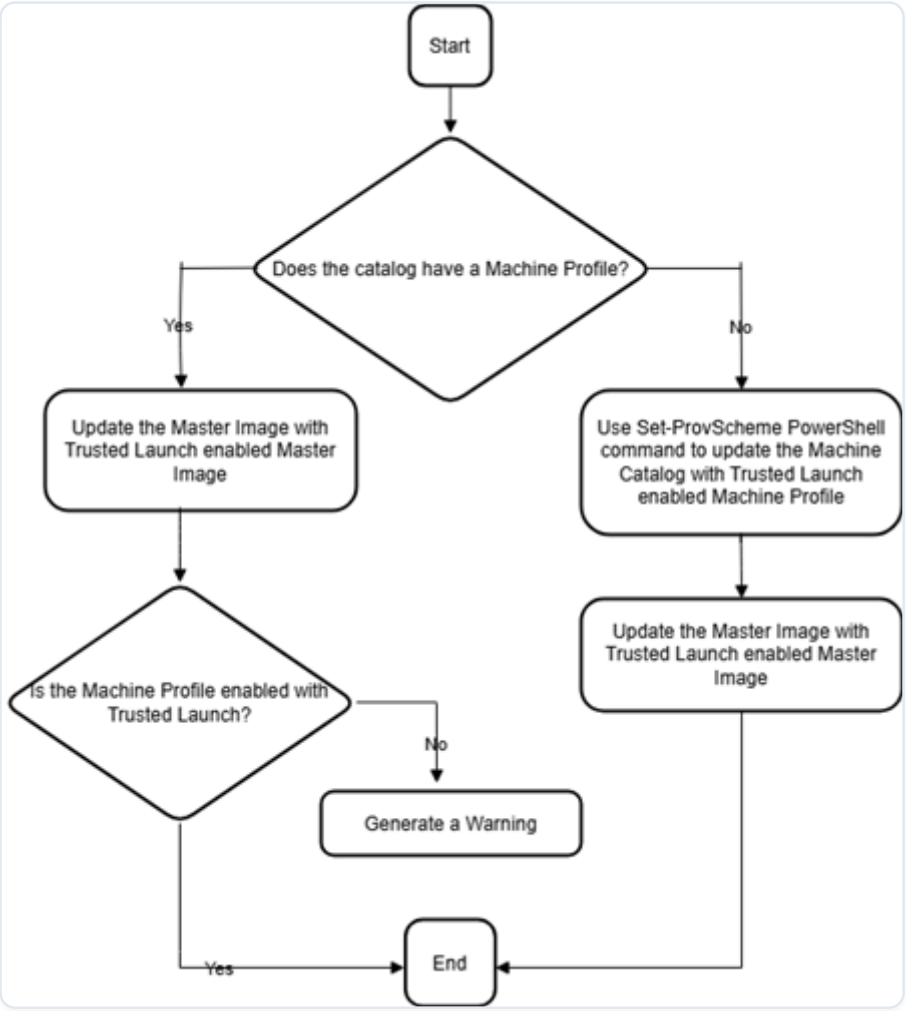
[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

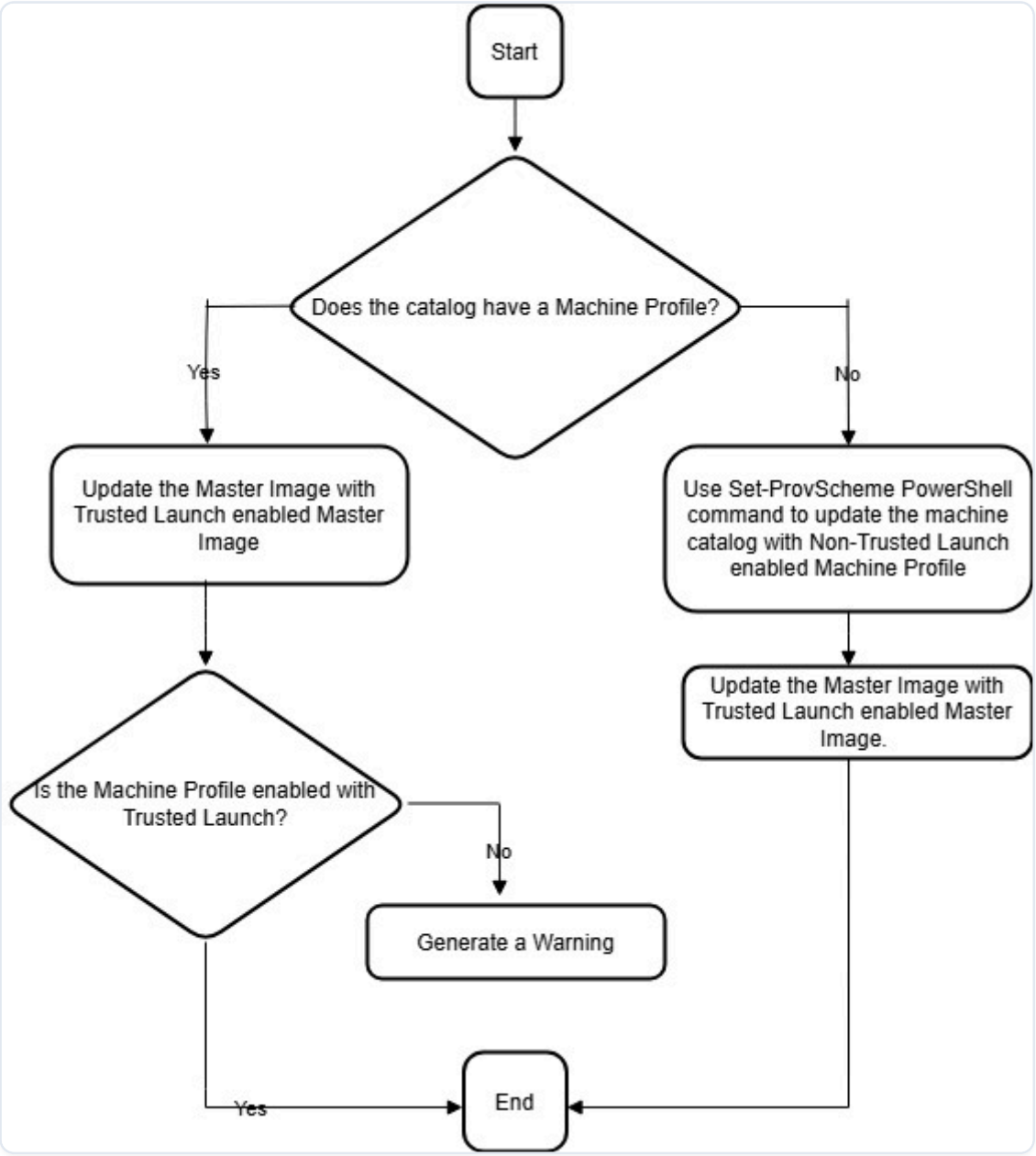
Atualizar um catálogo de máquinas com o Trusted Launch

Você pode atualizar catálogos de máquinas persistentes e não persistentes:

Para catálogo de máquinas persistente:



Para catálogo de máquinas não persistente:



Erros ao criar catálogos de máquinas com o Trusted Launch

Você recebe erros apropriados nos seguintes cenários ao criar um catálogo de máquinas com o Trusted Launch:

CENÁRIO	ERRO
Se você selecionar um perfil de máquina ao criar um catálogo não gerenciado	`MachineProfileNotSupportedForUnmanagedCatalog`
Se você selecionar um perfil de máquina que suporte Inicialização Confiável ao criar um catálogo com disco não gerenciado como imagem mestre	`SecurityTypeNotSupportedForUnmanagedDisk`

CENÁRIO	ERRO
Se você selecionar um perfil de máquina com um tipo de segurança diferente do tipo de segurança da imagem mestre	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`
Se você selecionar um tamanho de VM que não suporte Inicialização Confiável, mas usar uma imagem mestre que suporte Inicialização Confiável ao criar um catálogo	`MachineSizeNotSupportTrustedLaunch`

Usar valores de propriedade do perfil de máquina

O catálogo de máquinas usa as seguintes propriedades que são definidas nas propriedades personalizadas:

- Zona de disponibilidade
- ID do Grupo de Host Dedicado
- ID do Conjunto de Criptografia de Disco
- Tipo de SO
- Tipo de licença
- Tipo de armazenamento

Se essas propriedades personalizadas não forem definidas explicitamente, os valores das propriedades serão definidos a partir da especificação do modelo ARM ou da VM, o que for usado como perfil da máquina. Além disso, se `ServiceOffering` não for especificado, ele será definido a partir do perfil da máquina.

> **Nota:**

> Se algumas das propriedades estiverem ausentes do perfil da máquina e não forem definidas nas propriedades personalizadas, os valores padrão das propriedades serão aplicados onde for cabível.

> A seção a seguir descreve alguns cenários em `New-ProvScheme` e `Set-ProvScheme` quando `CustomProperties` têm todas as propriedades definidas ou os valores são derivados do MachineProfile.

- Cenários do New-ProvScheme
  - MachineProfile tem todas as propriedades e CustomProperties não estão definidas. Exemplo:

    `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

    Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

    ```
    Get-ProvScheme | select CustomProperties

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">

    <Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
    value>"/>

    <Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
    value>"/>

    <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
    value>"/>

    </CustomProperties>
    ```

  - MachineProfile tem algumas propriedades e CustomProperties não estão definidas. Exemplo: MachineProfile tem apenas LicenseType e OsType.

    `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

    Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

</CustomProperties>
```

- Tanto MachineProfile quanto CustomProperties definem todas as propriedades. Exemplo:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

As propriedades personalizadas têm prioridade. Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
```

```
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- Algumas propriedades são definidas em MachineProfile e algumas propriedades são definidas em CustomProperties. Exemplo:
  - CustomProperties definem LicenseType e StorageAccountType
  - MachineProfile define LicenseType, OsType e Zones

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- Algumas propriedades são definidas em MachineProfile e algumas propriedades são definidas em CustomProperties. Além disso, ServiceOffering não é definido. Exemplo:

- CustomProperties definem StorageType
- MachineProfile especifica LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>

</CustomProperties>
```

- Se o OsType não estiver nem em CustomProperties nem em MachineProfile, então:
  - O valor é lido da imagem mestre.
  - Se a imagem mestre for um disco não gerenciado, o OsType é definido como Windows. Exemplo:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

O valor da imagem mestre é gravado nas propriedades personalizadas, neste caso Linux.

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Cenários de Set-ProvScheme
  - Um catálogo existente com:
    - Propriedades Personalizadas para `StorageAccountType` e OsType
    - Perfil da Máquina `mpA.vm` que define zonas
  - Atualizações:
    - Perfil da Máquina mpB.vm que define StorageAccountType
    - Um novo conjunto de propriedades personalizadas $CustomPropertiesB que define LicenseType e OsType

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- Um catálogo existente com:
  - Propriedades Personalizadas para `StorageAccountType` e OsType
  - Perfil da Máquina `mpA.vm` que define StorageAccountType e LicenseType
- Atualizações:
  - Um novo conjunto de propriedades personalizadas $CustomPropertiesB que define StorageAccountType e OsType.

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-
value>"/>

</CustomProperties>
```

- Um catálogo existente com:
  - CustomProperties para `StorageAccountType` e OsType
  - MachineProfile `mpA.vm` que define Zonas
- Atualizações:
  - Um MachineProfile mpB.vm que define StorageAccountType e LicenseType
  - `ServiceOffering` não é especificado

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

Os seguintes valores são definidos como propriedades personalizadas para o catálogo:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-
value>"/>

</CustomProperties>
```

Configurar Zonas de Disponibilidade usando PowerShell

Usando o PowerShell, você pode visualizar os itens de inventário da oferta do Citrix DaaS usando `Get-Item`. Por exemplo, para visualizar a oferta de serviço da *região Leste dos EUA* `Standard_B1ls`:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

Para visualizar as zonas, use o parâmetro `AdditionalData` para o item:

`$serviceOffering.AdditionalData`

Se as Zonas de Disponibilidade não forem especificadas, não haverá alteração na forma como as máquinas são provisionadas.

Para configurar Zonas de Disponibilidade via PowerShell, use a propriedade personalizada **Zones** disponível com a operação `New-ProvScheme`. A propriedade **Zones** define uma lista de Zonas de Disponibilidade para provisionar máquinas. Essas zonas podem incluir uma ou mais Zonas de Disponibilidade. Por exemplo, `<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>` para as Zonas 1 e 3.

Use o comando `Set-ProvScheme` para atualizar as zonas de um esquema de provisionamento.

Se uma zona inválida for fornecida, o esquema de provisionamento não será atualizado e uma mensagem de erro aparecerá fornecendo instruções sobre como corrigir o comando inválido.

> **Dica:**
>
> Se você especificar uma propriedade personalizada inválida, o esquema de provisionamento não será atualizado e uma mensagem de erro relevante aparecerá.

Resultado do uso de grupos de host e zonas de disponibilidade do Azure ao mesmo tempo

Há uma verificação preliminar para avaliar se a criação de um catálogo de máquinas será bem-sucedida com base na zona de disponibilidade especificada na propriedade personalizada e na zona do grupo de host. A criação do catálogo falha se a propriedade personalizada da zona de disponibilidade não corresponder à zona do grupo de host.

Para obter informações sobre como configurar zonas de disponibilidade por meio do PowerShell, consulte Configuring Availability Zones through PowerShell.

Para obter informações sobre hosts dedicados do Azure, consulte Azure dedicated hosts.

A tabela a seguir descreve as várias combinações de zona de disponibilidade e zona de grupo de host e quais resultam na criação bem-sucedida ou falha de um catálogo de máquinas.

ZONA DO GRUPO DE HOST	ZONA DE DISPONIBILIDADE NA PROPRIEDADE PERSONALIZADA	RESULTADO DA CRIAÇÃO DO CATÁLOGO DE MÁQUINAS
Especificado. Por exemplo, o grupo de host está na Zona 1	Não especificado	Bem-sucedido. As máquinas são criadas na zona do grupo de host
Especificado. Por exemplo, o grupo de host está na Zona 1	Mesma zona que a zona do grupo de host. Por exemplo, a zona na propriedade personalizada está definida como 1	Bem-sucedido. As máquinas são criadas na Zona 1
Especificado. Por exemplo, o grupo de hosts está na Zona 1	Diferente da zona do grupo de hosts. Por exemplo, a zona na propriedade personalizada está definida como 2	Como a zona de disponibilidade especificada e a zona do grupo de hosts não correspondem, a criação do catálogo falha com um erro relevante durante as verificações pré-voo
Especificado. Por exemplo, o grupo de hosts está na Zona 1	Várias zonas especificadas. Por exemplo, as zonas nas propriedades personalizadas estão definidas como 1,2 ou 2,3	Como a zona de disponibilidade especificada e a zona do grupo de hosts não correspondem, a criação do catálogo falha com um erro relevante durante as verificações pré-voo
Não especificado. Por exemplo, a zona do grupo de hosts é `None`	Não especificado	Como a zona de disponibilidade especificada e a zona do grupo de hosts correspondem (ou seja, nenhuma zona), a criação do catálogo é bem-sucedida. As

ZONA DO GRUPO DE HOST	ZONA DE DISPONIBILIDADE NA PROPRIEDADE PERSONALIZADA	RESULTADO DA CRIAÇÃO DO CATÁLOGO DE MÁQUINAS
		máquinas não são criadas em nenhuma zona
Não especificado. Por exemplo, a zona do grupo de hosts é `None`	Especificado. Por exemplo, as zonas na propriedade personalizada estão definidas como uma ou várias zonas	Como a zona de disponibilidade especificada e a zona do grupo de hosts não correspondem, a criação do catálogo falha com um erro relevante durante as verificações pré-voo

Provisionar VMs em hosts dedicados do Azure

Você pode usar o MCS para provisionar VMs em hosts dedicados do Azure. Antes de provisionar VMs em hosts dedicados do Azure:

- Criar um grupo de hosts.
- Criar hosts nesse grupo de hosts.
- Certifique-se de que há capacidade de host suficiente reservada para a criação de catálogos e máquinas virtuais.

Você pode criar um catálogo de máquinas com locação de host definida através do seguinte script PowerShell:

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

Ao usar o MCS para provisionar máquinas virtuais em hosts dedicados do Azure, considere:

- Um *host dedicado* é uma propriedade do catálogo e não pode ser alterado depois que o catálogo é criado. A locação dedicada não é atualmente suportada no Azure.
- Um grupo de hosts do Azure pré-configurado, na região da unidade de hospedagem, é necessário ao usar o parâmetro `HostGroupId`.
- O posicionamento automático do Azure é necessário. Essa funcionalidade faz uma solicitação para integrar a assinatura associada ao grupo de hosts. Para obter mais informações, consulte VM Scale Set on Azure Dedicated Hosts - Public Preview. Se o posicionamento automático não estiver habilitado, o MCS gerará um erro durante a criação do catálogo.

Configurar tipos de armazenamento

Selecione diferentes tipos de armazenamento para máquinas virtuais em ambientes Azure que usam MCS. Para VMs de destino, o MCS suporta:

- Disco do SO: SSD premium, SSD ou HDD
- Disco de cache de write-back: SSD premium, SSD ou HDD

Ao usar esses tipos de armazenamento, considere o seguinte:

- Certifique-se de que sua VM suporta o tipo de armazenamento selecionado.
- Se sua configuração usa um disco efêmero do Azure, você não terá a opção de configuração de disco de cache de write-back.

> **Dica:**

> `StorageType` é configurado para um tipo de SO e conta de armazenamento. `WBCDiskStorageType` é configurado para o tipo de armazenamento de cache de write-back. Para um catálogo normal, `StorageType` é necessário. Se `WBCDiskStorageType` não estiver configurado, `StorageType` é usado como padrão para `WBCDiskStorageType`.

> Se WBCDiskStorageType não estiver configurado, então StorageType é usado como padrão para WBCDiskStorageType

Configurar tipos de armazenamento para VMs

Para configurar tipos de armazenamento para VMs, use o parâmetro `StorageType` em `New-ProvScheme`. Para atualizar o valor do parâmetro `StorageType` em um catálogo existente para um dos tipos de armazenamento suportados, use o comando `Set-ProvScheme`.

A seguir, um exemplo de conjunto do parâmetro `CustomProperties` em um esquema de provisionamento:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

Habilitar armazenamento com redundância de zona

Você pode selecionar o armazenamento com redundância de zona durante a criação do catálogo. Ele replica seu disco gerenciado do Azure de forma síncrona em várias zonas de disponibilidade, o que permite que você se recupere de uma falha em uma zona utilizando a redundância em outras.

Você pode especificar **Premium_ZRS** e **StandardSSD_ZRS** nas propriedades personalizadas do tipo de armazenamento. O armazenamento ZRS pode ser configurado usando propriedades personalizadas existentes ou através do modelo **MachineProfile**. O armazenamento ZRS também é suportado com o comando `Set-ProvVMUpdateTimeWindow` com os parâmetros `-StartsNow` e `-DurationInMinutes -1`. Você pode alterar VMs existentes de armazenamento LRS para ZRS.

Nota:

- `StartsNow` indica que o horário de início agendado é o horário atual.
- `DurationInMinutes` com um número negativo (por exemplo, –1) indica que não há limite superior na janela de tempo do agendamento.

Limitações:

- Suportado apenas para discos gerenciados
- Suportado apenas com unidades de estado sólido (SSD) premium e padrão
- Não compatível com `StorageTypeAtShutdown`
- Disponível apenas em certas regiões.
- O desempenho do Azure diminui ao criar discos ZRS em escala. Portanto, para a primeira inicialização, ligue as máquinas em lotes menores (menos de 300 máquinas por vez)

Definir o armazenamento com redundância de zona como o tipo de armazenamento de disco

Você pode selecionar o armazenamento com redundância de zona durante a criação inicial do catálogo, ou pode atualizar seu tipo de armazenamento em um catálogo existente.

Selecionar armazenamento com redundância de zona usando comandos do PowerShell

Ao criar um novo catálogo no Azure usando o comando PowerShell `New-ProvScheme`, use `Standard_ZRS` como valor em `StorageAccountType`. Por exemplo:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

Ao definir esse valor, ele é validado por uma API dinâmica que determina se pode ser usado corretamente. As seguintes exceções podem ocorrer se o uso de ZRS não for válido para o seu catálogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: A propriedade personalizada StorageTypeAtShutdown não pode ser usada com o armazenamento ZRS.
- **StorageAccountTypeNotSupportedInRegion**: Essa exceção ocorre se você tentar usar o armazenamento ZRS em uma região do Azure que não oferece suporte a ZRS.
- **ZrsRequiresManagedDisks**: Você pode usar o armazenamento com redundância de zona somente com discos gerenciados.

Você pode definir o tipo de armazenamento de disco usando as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Nota:**
>
> Durante a criação do catálogo, o disco do SO do perfil da máquina `StorageType` é usado se as propriedades personalizadas não estiverem definidas.

Capturar configurações de diagnóstico em VMs e NICs de um perfil de máquina

Você pode capturar configurações de diagnóstico em VMs e NICs de um perfil de máquina ao criar um catálogo de máquinas, atualizar um catálogo de máquinas existente e atualizar VMs existentes.

Você pode criar uma VM ou especificação de modelo como uma fonte de perfil de máquina.

Etapas principais

1. Configure os IDs necessários no Azure. Você deve fornecer esses IDs na especificação do modelo.
    - Conta de armazenamento
    - Espaço de trabalho do Log Analytics
    - Namespace do hub de eventos com o preço da camada padrão
2. Criar fonte de perfil de máquina.
3. Crie um novo catálogo de máquinas, atualize um catálogo existente ou atualize VMs existentes.

Configurar IDs necessárias no Azure

Configure um dos seguintes no Azure:

- Conta de armazenamento
- Espaço de trabalho do Log Analytics
- Namespace do Hub de Eventos com o preço da camada Standard

CONFIGURAR UMA CONTA DE ARMAZENAMENTO

Crie uma conta de armazenamento padrão no Azure. Na especificação do modelo, forneça o resourceId completo para a conta de armazenamento como o `storageAccountId`.

Depois que as VMs são configuradas para registrar dados na conta de armazenamento, os dados podem ser encontrados no contêiner `insights-metrics-pt1m`.

CONFIGURAR UM ESPAÇO DE TRABALHO DO LOG ANALYTICS

Crie um espaço de trabalho do Log Analytics. Na especificação do modelo, forneça o resourceId completo para o espaço de trabalho do Log Analytics como o workspaceId.

Depois que as VMs são configuradas para registrar dados no espaço de trabalho, os dados podem ser consultados em Logs no Azure. Você pode executar o seguinte comando no Azure em Logs para mostrar uma contagem de todas as métricas registradas por um recurso:

```
AzureMetrics | summarize Count=count() by ResourceId
```

CONFIGURAR UM HUB DE EVENTOS

Faça o seguinte para configurar um hub de eventos no portal do Azure:

1. Crie um namespace do hub de eventos com o preço da camada padrão.
2. Crie um hub de eventos sob o namespace.
3. navegar para **Captura** sob o hub de eventos. Ative o botão para capturar com o tipo de saída Avro.
4. Crie um novo contêiner em uma conta de armazenamento existente para capturar os logs.
5. Na especificação do modelo, especifique o `eventHubAuthorizationRuleId` no seguinte formato: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Especifique o nome do hub de eventos.

Depois que as VMs são configuradas para registrar dados no hub de eventos, os dados são capturados no contêiner de armazenamento configurado.

Criar uma origem de perfil de máquina

Você pode criar uma VM ou especificação de modelo como uma origem de perfil de máquina.

CRIAR UM PERFIL DE MÁQUINA BASEADO EM VM COM CONFIGURAÇÕES DE DIAGNÓSTICO

Se você quiser criar uma VM como seu perfil de máquina, então primeiro configure as configurações de diagnóstico na própria VM do modelo. Você pode consultar as instruções detalhadas fornecidas na documentação da Microsoft Configurações de diagnóstico no Azure Monitor.

Você pode executar os seguintes comandos para verificar se agora há configurações de diagnóstico associadas à VM ou NIC:

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

CRIAR UM PERFIL DE MÁQUINA BASEADO EM ESPECIFICAÇÃO DE MODELO COM CONFIGURAÇÕES DE DIAGNÓSTICO

Se você quiser usar uma VM que já tenha as configurações de diagnóstico habilitadas e exportá-la para uma especificação de modelo ARM, essas configurações não serão incluídas automaticamente no modelo. Você deve adicionar ou modificar manualmente as configurações de diagnóstico dentro do modelo ARM.

No entanto, se você quiser uma VM como seu perfil de máquina, o MCS garante que as configurações de diagnóstico críticas sejam capturadas com precisão e aplicadas aos recursos dentro do seu catálogo MCS.

1. Crie uma especificação de modelo padrão que define uma VM e NICs.
2. Adicione recursos adicionais para implantar as configurações de diagnóstico de acordo com a especificação: Microsoft.Insights diagnosticSettings. Para o escopo, faça referência a uma VM ou NIC que esteja no modelo pelo nome com um ID parcial. Por exemplo, para criar configurações de diagnóstico anexadas a uma VM chamada test-VM na especificação do modelo, especifique o escopo como:

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. Use a especificação do modelo como uma origem de perfil de máquina.

Criar ou atualizar um catálogo com configurações de diagnóstico

Depois de criar uma origem de perfil de máquina, agora você pode criar um catálogo de máquinas usando o comando `New-ProvScheme`, atualizar um catálogo de máquinas existente usando o comando `Set-ProvScheme` e atualizar VMs existentes usando o comando `Request-ProvVMUpdate`.

Verificar a licença do Windows

Você pode verificar se a VM provisionada está usando o benefício de licenciamento executando o seguinte comando PowerShell: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Para o tipo de licença do Windows Server, verifique se o tipo de licença é **Windows_Server**. Mais instruções estão disponíveis em `<https://docs.microsoft.com/pt-br/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>`.
- Para o tipo de licença do Windows Client, verifique se o tipo de licença é **Windows_Client**. Mais instruções estão disponíveis em `<https://docs.microsoft.com/pt-br/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>`.

Alternativamente, você pode usar o SDK do PowerShell `Get-Provscheme` para fazer a verificação. Por exemplo: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Para obter mais informações sobre este cmdlet, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>`.

Configurar a licença do Linux

Com as licenças Linux bring-your-own-subscription (BYOS), você não precisa pagar pelo software. A cobrança BYOS inclui apenas a taxa de hardware de computação. Existem dois tipos de licenças:

- **RHEL_BYOS**: Para usar o tipo RHEL_BYOS com sucesso, habilite o Red Hat Cloud Access em sua assinatura do Azure.
- **SLES_BYOS**: As versões BYOS do SLES incluem suporte da SUSE.

Você pode definir o valor de LicenseType para as opções do Linux em `New-ProvScheme` e `Set-ProvScheme`.

Exemplo de configuração de LicenseType para RHEL_BYOS em `New-ProvScheme`:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

Exemplo de configuração de LicenseType para SLES_BYOS em `Set-ProvScheme`:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="SLES_BYOS" /></CustomProperties>'
```

Nota:

Se o valor `LicenseType` estiver vazio, os valores padrão serão Licença do Azure Windows Server ou Licença do Azure Linux, dependendo do valor de OsType.

Exemplo de como definir LicenseType como vazio:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

Criar um catálogo de máquinas com um disco efêmero do Azure

Para provisionar discos de SO efêmeros usando `New-ProvScheme`, considere as seguintes restrições:

- O tamanho da VM usado para o catálogo deve suportar discos de SO efêmeros.
- O tamanho do cache ou do disco temporário associado ao tamanho da VM deve ser maior ou igual ao tamanho do disco do SO.
- O tamanho do disco temporário deve ser maior que o tamanho do disco de cache.

Considere também estas restrições ao:

- Criar o esquema de provisionamento
- Modificar o esquema de provisionamento
- Atualizar a imagem

Para usar discos efêmeros, você deve definir a propriedade personalizada `UseEphemeralOsDisk` como **true** ao executar `New-ProvScheme`.

> **Nota:**
>
> Se a propriedade personalizada `UseEphemeralOsDisk` for definida como **false** ou um valor não for especificado, todos os VDAs provisionados continuarão a usar um disco de SO provisionado.

> A seguir, um exemplo de conjunto de propriedades personalizadas a serem usadas no esquema de provisionamento:

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },

            {

                "Name": "StorageType",

                "Value": "Standard_LRS"

            },

            {

                "Name": "UseSharedImageGallery",
```

```
                "Value": "true"
            },
            {
                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
            },
            {
                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
            },
            {
                "Name": "LicenseType",
                "Value": "Windows_Server"
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

Configurar um disco efêmero para um catálogo existente

Para configurar um disco de SO efêmero do Azure para um catálogo existente, use o parâmetro `UseEphemeralOsDisk` em `Set-ProvScheme`. Defina o valor do parâmetro `UseEphemeralOsDisk` como **true**.

> **Nota:**
>
> Para usar este recurso, você também deve habilitar os parâmetros `UseManagedDisks` e `UseSharedImageGallery`.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

Configurar tipo de armazenamento usado por discos efêmeros

Por padrão, `Standard_LRS` é o tipo de armazenamento usado pelo recurso de disco de SO efêmero. Você pode definir o tipo de armazenamento para usar SSDs em vez disso para aumentar os IOPS do disco em operações de leitura, especificando a propriedade personalizada `StorageType`. Os valores suportados atualmente são `Standard_LRS`, `StandardSSD_LRS` e `Premium_LRS`.

`StorageType` também pode ser atualizado em máquinas efêmeras existentes com `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`.

Configurar Galeria de Computação do Azure

Use o comando `New-ProvScheme` para criar um esquema de provisionamento com suporte à Galeria de Computação do Azure. Use o comando `Set-ProvScheme` para habilitar ou desabilitar este recurso para um esquema de provisionamento e para alterar a taxa de réplicas e os valores máximos de réplicas.

Três propriedades personalizadas foram adicionadas aos esquemas de provisionamento para suportar o recurso Galeria de Computação do Azure:

`UseSharedImageGallery`

- Define se a Galeria de Computação do Azure deve ser usada para armazenar as imagens publicadas. Se definido como **True**, a imagem é armazenada como uma imagem da Galeria de Computação do Azure; caso contrário, a imagem é armazenada como um instantâneo.
- Os valores válidos são **True** e **False**.
- Se a propriedade não for definida, o valor padrão é **False**.

`SharedImageGalleryReplicaRatio`

- Define a proporção de máquinas para réplicas da versão da imagem da galeria.
- Os valores válidos são números inteiros maiores que 0.
- Se a propriedade não for definida, os valores padrão são usados. O valor padrão para discos de SO persistentes é 1000 e o valor padrão para discos de SO não persistentes é 40.

`SharedImageGalleryReplicaMaximum`

- Define o número máximo de réplicas para cada versão da imagem da galeria.
- Os valores válidos são números inteiros maiores que 0 e até 100. O MCS gera um erro se você fornecer um valor fora do intervalo válido.
- Se a propriedade não for definida, o valor padrão é 10.
- Se a propriedade não for definida, o valor padrão é 100.

> **Dica:**

> Ao usar a Galeria de Computação do Azure para armazenar uma imagem publicada para catálogos provisionados pelo MCS, o MCS define a contagem de réplicas da versão da imagem da galeria com base no número de máquinas no catálogo, na proporção de réplicas e no máximo de réplicas. A contagem de réplicas é calculada dividindo o número de

> máquinas no catálogo pela proporção de réplicas (arredondando para o valor inteiro mais próximo) e, em seguida, limitando o valor à contagem máxima de réplicas. Por exemplo, com uma proporção de réplicas de 20 e um máximo de 5, 0 a 20 máquinas têm uma réplica criada, 21 a 40 têm 2 réplicas, 41 a 60 têm 3 réplicas, 61 a 80 têm 4 réplicas, 81+ têm 5 réplicas.

Caso de uso: Atualizando a proporção de réplicas e o máximo de réplicas da Galeria de Computação do Azure

O catálogo de máquinas existente usa a Galeria de Computação do Azure. Use o comando `Set-ProvScheme` para atualizar as propriedades personalizadas para todas as máquinas existentes no catálogo e quaisquer máquinas futuras:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

Caso de uso: Convertendo um catálogo de instantâneos em um catálogo da Galeria de Computação do Azure

Para este caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **True**. Opcionalmente, inclua as propriedades `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum`.
2. Atualize o catálogo.
3. Reinicie as máquinas para forçar uma atualização.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

Dica:

Os parâmetros `SharedImageGalleryReplicaRatio` e `SharedImageGalleryReplicaMaximum` não são necessários. Após a conclusão do comando `Set-ProvScheme`, a imagem da Galeria de Computação do Azure ainda não foi criada. Depois que o catálogo é configurado para usar a galeria, a próxima operação de atualização do catálogo armazena a imagem publicada na galeria. O comando de atualização do catálogo cria a galeria, a imagem da galeria e a versão da imagem. Reiniciar as máquinas as atualiza, momento em que a contagem de réplicas é atualizada, se apropriado. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando a imagem da Galeria de Computação do Azure e todas as máquinas recém-provisionadas são criadas usando a imagem. O instantâneo antigo é limpo automaticamente em algumas horas.

Caso de uso: Convertendo um catálogo da Galeria de Computação do Azure para um catálogo de instantâneos

Para este caso de uso:

1. Execute `Set-ProvScheme` com o sinalizador `UseSharedImageGallery` definido como **False** ou não definido.
2. Atualize o catálogo.
3. Reinicie as máquinas para forçar uma atualização.

Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
```

```
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

Dica:

Ao contrário da atualização de um instantâneo para um catálogo da Galeria de Computação do Azure, os dados personalizados para cada máquina ainda não foram atualizados para refletir as novas propriedades personalizadas. Execute o seguinte comando para ver as propriedades personalizadas originais da Galeria de Computação do Azure: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Após a conclusão do comando `Set-ProvScheme`, o instantâneo da imagem ainda não foi criado. Depois que o catálogo é configurado para não usar a galeria, a próxima operação de atualização do catálogo armazena a imagem publicada como um instantâneo. A partir desse momento, todas as máquinas não persistentes existentes são redefinidas usando o instantâneo e todas as máquinas recém-provisionadas são criadas a partir do instantâneo. Reiniciar as máquinas as atualiza, momento em que os dados personalizados da máquina são atualizados para refletir que `UseSharedImageGallery` está definido como **False**. Os ativos antigos da Galeria de Computação do Azure (galeria, imagem e versão) são limpos automaticamente em algumas horas.

Criar ou atualizar um catálogo com várias NICs por VM

O MCS oferece suporte a várias NICs por VM. Você pode associar várias NICs em uma VM a várias sub-redes, no entanto, essas sub-redes devem estar na mesma rede virtual (VNet). Você pode usar o comando PowerShell para:

- Criar um catálogo com várias NICs em uma VM
- Atualizar uma configuração de catálogo existente para ter várias NICs em uma VM, de modo que as VMs recém-criadas tenham várias NICs
- Atualizar uma VM existente para ter várias NICs

Você pode criar ou atualizar um catálogo de máquinas baseado em perfil não-máquina e um catálogo de máquinas baseado em perfil de máquina para ter várias NICs em uma VM. Atualmente, para um catálogo de máquinas baseado em perfil de máquina, você só pode ter o mesmo número de NICs especificado na origem do perfil da máquina.

Propriedades como rede acelerada são derivadas da origem do perfil da máquina.

> **Nota:**
>
> O tamanho da VM deve suportar o mesmo número de NICs e a rede acelerada correspondente, caso contrário, você receberá um erro.

> Você pode recuperar o número máximo de NICs associadas a um tamanho de VM selecionado. Uma propriedade do PowerShell chamada `MaxNetworkInterfaces` exibe a contagem máxima de NICs ao executar o comando do PowerShell `get-item` com o parâmetro `AdditionalData`.

Recuperar a contagem máxima de NICs

Para recuperar a contagem máxima de NICs:

1. Abra uma janela do **PowerShell** no host do Delivery Controller™.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Execute `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"` para listar todos os tamanhos de VM disponíveis.
4. Execute `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData`
5. Verifique `MaxNetworkInterfaces` para saber a contagem máxima de NICs.

Criar um catálogo com várias NICs em uma VM

Para criar um catálogo com várias NICs em uma VM, faça o seguinte:

1. Abra uma janela do PowerShell a partir do host do Delivery Controller.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um pool de identidades, se ainda não tiver sido criado.
4. Crie o esquema de provisionamento:

   - Se estiver criando um catálogo de máquinas não baseado em perfil de máquina, execute o comando `New-ProvScheme` com o parâmetro `NetworkMappings`. Você pode adicionar várias sub-redes ao parâmetro `NetworkMappings`. Por exemplo:

     ```
     New-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

- Se estiver criando um catálogo de máquinas baseado em perfil de máquina:

  a. Crie uma VM no Azure para ter várias NICs. Para obter informações, consulte Criar e gerenciar uma máquina virtual Windows com várias NICs. Você também pode criar uma nova VM e, em seguida, anexar uma interface de rede na página Rede do portal do Azure.

  b. Execute o comando `New-ProvScheme` com a VM como entrada de perfil de máquina.

> **Nota:**
>
> Ao criar um catálogo de máquinas baseado em perfil de máquina, a contagem de `NetworkMappings` deve ser a mesma que a `NetworkInterfaceCount` do perfil de máquina. O `NetworkInterfaceCount` pode ser recuperado de `AdditionalData` de `Get-item -Path "machine profile path"`.

5. Conclua a criação do catálogo.

Atualizar um catálogo para ter várias NICs em uma VM

Para atualizar um catálogo para ter várias NICs em uma VM, faça o seguinte:

1. Abra uma janela do **PowerShell** no host do Delivery Controller.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Atualize o esquema de provisionamento:

   - Se estiver criando um catálogo de máquinas não baseado em perfil de máquina, execute o comando `Set-ProvScheme` com o parâmetro `NetworkMappings`. Você pode adicionar várias sub-redes ao parâmetro `NetworkMappings`. Por exemplo:

     ```
     Set-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - Se estiver criando um catálogo de máquinas baseado em um perfil de máquina:

     a. Crie uma VM no Azure para ter várias NICs. Para obter informações, consulte Criar e gerenciar uma máquina virtual Windows com várias NICs.

     b. Execute o comando `Set-ProvScheme` com a VM como entrada de perfil de máquina.

Atualizar uma VM existente para ter várias NICs em uma VM

Você também pode atualizar uma VM existente usando `Set-ProvVMUpdateTimeWindow` e também realizar um ciclo de energia na VM existente durante a janela de tempo de atualização. Para obter mais informações sobre como atualizar uma VM existente, consulte Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento.

Criar um catálogo de máquinas com disco de cache de write-back não persistente

Para configurar um catálogo com disco de cache de write-back não persistente, use o parâmetro PowerShell `New-ProvScheme CustomProperties`. As propriedades personalizadas são:

- `UseTempDiskForWBC`. Esta propriedade indica se você aceita usar o armazenamento temporário do Azure para armazenar o arquivo de cache de write-back. Isso deve ser configurado como true ao executar `New-ProvScheme` se você quiser usar o disco temporário como disco de cache de write-back. Se esta propriedade não for especificada, o parâmetro será definido como False por padrão.

Por exemplo, usando o parâmetro `CustomProperties` para definir `UseTempDiskForWBC` como true:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `
```

```
</CustomProperties>'
```

Nota:

Depois de confirmar o catálogo de máquinas para usar o armazenamento temporário local do Azure para o arquivo de cache de write-back, ele não poderá ser alterado para usar VHD posteriormente.

Criar um catálogo de máquinas com disco de cache de write-back persistente

Para configurar um catálogo com disco de cache de write-back persistente, use o parâmetro PowerShell `New-ProvScheme CustomProperties`.

Dica:

Use o parâmetro PowerShell `New-ProvScheme CustomProperties` apenas para conexões de hospedagem baseadas em nuvem. Se você quiser provisionar máquinas usando um disco de cache de write-back persistente para uma solução local (por exemplo, XenServer®), o PowerShell não é necessário porque o disco persiste automaticamente.

Este parâmetro suporta uma propriedade extra, `PersistWBC`, usada para determinar como o disco de cache de write-back persiste para máquinas provisionadas por MCS. A propriedade `PersistWBC` é usada apenas quando o parâmetro `UseWriteBackCache` é especificado e quando o parâmetro `WriteBackCacheDiskSize` é definido para indicar que um disco é criado.

Nota:

Este comportamento se aplica tanto ao Azure quanto ao GCP, onde o disco de cache de write-back MCSIO padrão é excluído e recriado ao reiniciar. Você pode optar por persistir o disco para evitar a exclusão e recriação do disco de cache de write-back MCSIO.

Exemplos de propriedades encontradas no parâmetro `CustomProperties` antes de suportar `PersistWBC` incluem:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

Nota:

Este exemplo se aplica apenas ao Azure. As propriedades são diferentes no ambiente GCP.

Ao usar essas propriedades, considere que elas contêm valores padrão se as propriedades forem omitidas do parâmetro `CustomProperties`. A propriedade `PersistWBC` tem dois valores possíveis: **true** ou **false**.

Definir a propriedade `PersistWBC` como **true** não exclui o disco de cache de write-back quando o administrador do Citrix DaaS desliga a máquina da interface de gerenciamento.

Definir a propriedade `PersistWBC` como **false** exclui o disco de cache de write-back quando o administrador do Citrix DaaS desliga a máquina da interface de gerenciamento.

Nota:

Se a propriedade `PersistWBC` for omitida, a propriedade assume o valor padrão **false** e o cache de write-back é excluído quando a máquina é desligada da interface de gerenciamento.

Por exemplo, usando o parâmetro `CustomProperties` para definir `PersistWBC` como verdadeiro:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

Importante:

A propriedade `PersistWBC` só pode ser definida usando o cmdlet do PowerShell `New-ProvScheme`. Tentar alterar o `CustomProperties` de um esquema de provisionamento após a criação não tem impacto no catálogo de máquinas e na persistência do disco de cache de write-back quando uma máquina é desligada.

Por exemplo, defina `New-ProvScheme` para usar o cache de write-back enquanto define a propriedade `PersistWBC` como verdadeira:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`" /
>

</CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Melhore o desempenho de inicialização com MCSIO

Você pode melhorar o desempenho de inicialização para discos gerenciados do Azure e GCP quando o MCSIO estiver habilitado. Use a propriedade personalizada do PowerShell `PersistOSDisk` no comando `New-ProvScheme` para configurar esse recurso. As opções associadas a `New-ProvScheme` incluem:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

Para habilitar esse recurso, defina a propriedade personalizada `PersistOSDisk` como **true**. Por exemplo:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}
```

```
-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

Criar um catálogo de máquinas com chave de criptografia gerenciada pelo cliente

Se você deseja criar um catálogo de máquinas usando comandos do PowerShell, onde a chave de criptografia é uma chave gerenciada pelo cliente, faça o seguinte:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos do PowerShell específicos da Citrix.
3. Digite `cd xdhyp:/`.
4. Digite `cd .\HostingUnits\(your hosting unit)`.
5. Digite cd diskencryptionset.folder.
6. Digite dir para obter a lista dos Conjuntos de Criptografia de Disco.
7. Copie o Id de um Conjunto de Criptografia de Disco.
8. Crie uma string de propriedade personalizada para incluir o Id do Conjunto de Criptografia de Disco. Por exemplo:

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. Crie um pool de identidades se ainda não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. Execute o comando New-ProvScheme: Por exemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"

-CustomProperties $customProperties
```

11. Conclua a criação do catálogo de máquinas.

Criar um catálogo de máquinas com capacidade de criptografia no host

Para criar um catálogo de máquinas com capacidade de criptografia no host

1. Verifique se a assinatura tem o recurso de criptografia no host habilitado ou não. Para fazer isso, consulte `<https://learn.microsoft.com/pt-br/rest/api/resources/features/get?tabs=HTTP/>`. Se não estiver habilitado, você deve habilitar o recurso para a assinatura. Para obter informações sobre como habilitar o recurso para sua assinatura, consulte `<https://learn.microsoft.com/pt-br/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`.
2. Verifique se um tamanho de VM específico do Azure suporta criptografia no host ou não. Para fazer isso, em uma janela do PowerShell, execute um dos seguintes:

   ```
   PS XDHyp:\Connections\<your connection>\east
   us.region\serviceoffering.folder>
   ```

   ```
   PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
   ```

3. Crie uma VM ou uma especificação de modelo, como entrada para o perfil da máquina, no portal do Azure com a criptografia no host habilitada.

   - Se você quiser criar uma VM, selecione um tamanho de VM que suporte criptografia no host. Depois de criar a VM, a propriedade da VM **Criptografia no host** é habilitada.
   - Se você quiser usar uma especificação de modelo, atribua o parâmetro `Encryption at Host` como **true** dentro de `securityProfile`.

4. Crie um catálogo de máquinas MCS com fluxo de trabalho de perfil de máquina, selecionando uma VM ou uma especificação de modelo.

   - Disco do SO / Disco de Dados: É criptografado por meio de chave gerenciada pelo cliente e chave gerenciada pela plataforma
   - Disco do SO Efêmero: É criptografado apenas por meio de chave gerenciada pela plataforma
   - Disco de Cache: É criptografado por meio de chave gerenciada pelo cliente e chave gerenciada pela plataforma

   Você pode criar o catálogo de máquinas usando o Studio ou executando comandos PowerShell.

Recuperar informações de criptografia no host de um perfil de máquina

Você pode recuperar as informações de criptografia no host de um perfil de máquina ao executar o comando PowerShell com o parâmetro `AdditionalData`. Se o parâmetro `EncryptionAtHost` for **True**, isso indica que a criptografia no host está habilitada para o perfil de máquina.

Por exemplo: Quando a entrada do perfil de máquina é uma VM, execute o seguinte comando:

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

Por exemplo: Quando a entrada do perfil de máquina é uma especificação de modelo, execute o seguinte comando:

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

Criar um catálogo de máquinas com criptografia dupla

Você pode criar e atualizar um catálogo de máquinas com criptografia dupla usando o Studio e comandos PowerShell.

As etapas detalhadas sobre como criar um catálogo de máquinas com criptografia dupla são:

1. Crie um Azure Key Vault e DES com chaves gerenciadas pela plataforma e pelo cliente. Para obter informações sobre como criar um Azure Key Vault e um DES, consulte Use o portal do Azure para habilitar a criptografia dupla em repouso para discos gerenciados.
2. Para procurar Conjuntos de Criptografia de Disco disponíveis em sua conexão de hospedagem:
    a. Abra uma janela do **PowerShell**.
    b. Execute os seguintes comandos PowerShell:
        i. `asnp citrix*`
        ii. `cd xdhyp:`:
        iii. `cd HostingUnits`

iv. `cd YourHostingUnitName (ex. azure-east)`

v. `cd diskencryptionset.folder`

vi. `dir`

Você pode usar um ID do `DiskEncryptionSet` para criar ou atualizar um catálogo usando propriedades personalizadas.

3. Se você quiser usar o fluxo de trabalho de perfil de máquina, crie uma VM ou especificação de modelo como entrada de perfil de máquina.

   - Se você quiser usar uma VM como entrada de perfil de máquina:

     a. Crie uma VM no Portal do Azure.

     b. navegar para **Discos>Gerenciamento de chaves** para criptografar a VM diretamente com qualquer `DiskEncryptionSetID`.

   - Se você quiser usar uma especificação de modelo como entrada de perfil de máquina:

     a. No modelo, em `properties>storageProfile>osDisk>managedDisk`, adicione o parâmetro `diskEncryptionSet` e adicione o ID do DES de criptografia dupla.

4. Crie o catálogo de máquinas.

   - Se estiver usando o Studio, faça um dos seguintes, além das etapas em Criar catálogos de máquinas.

     ◦ Se você não usar um fluxo de trabalho baseado em perfil de máquina, na página **Configurações de Disco**, selecione **Usar a seguinte chave para criptografar dados em cada máquina**. Em seguida, selecione seu DES de criptografia dupla na lista suspensa. Continue criando o catálogo.

     ◦ Se estiver usando o fluxo de trabalho de perfil de máquina, na página **Imagem**, selecione uma imagem mestre (ou imagem preparada) e um perfil de máquina. Certifique-se de que o perfil de máquina tenha um ID de conjunto de criptografia de disco em suas propriedades.

     Todas as máquinas criadas no catálogo são criptografadas duplamente pela chave associada ao DES que você selecionou.

   - Se estiver usando comandos do PowerShell, faça um dos seguintes:

- Se não estiver usando o fluxo de trabalho baseado em perfil de máquina, adicione a propriedade personalizada `DiskEncryptionSetId` no comando `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1

-MasterImageVM "Redacted"

-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- Se estiver usando o fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east
```

```
-IdentityPoolName aio-ip

-InitialBatchSizeHint 1

-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

Conclua a criação de um catálogo usando o SDK remoto do PowerShell. Todas as máquinas criadas no catálogo são criptografadas duplamente pela chave associada ao DES que você selecionou.

Converter um catálogo não criptografado para usar criptografia dupla

Você pode atualizar o tipo de criptografia de um catálogo de máquinas (usando propriedades personalizadas ou perfil de máquina).

- Se não estiver usando o fluxo de trabalho baseado em perfil de máquina, adicione a propriedade personalizada DiskEncryptionSetId no comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />
```

```
</CustomProperties>'
```

- Se estiver usando o fluxo de trabalho baseado em perfil de máquina, use uma entrada de perfil de máquina no comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

Após o sucesso, todas as novas VMs que você adicionar ao seu catálogo serão criptografadas duplamente pela chave associada ao DES que você selecionou.

Verificar se o catálogo está criptografado duplamente

- No Studio:
  a. navegar para **Catálogos de Máquinas**.
  b. Selecione o catálogo que você deseja verificar. Clique na guia **Propriedades do Modelo** localizada perto da parte inferior da tela.
  c. Em **Detalhes do Azure**, verifique o ID do Conjunto de Criptografia de Disco em **Conjunto de Criptografia de Disco**. Se o ID DES do catálogo estiver em branco, o catálogo não está criptografado.
  d. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES é de chaves gerenciadas pela plataforma e gerenciadas pelo cliente.
- Usando o comando PowerShell:
  a. Abra a janela do **PowerShell**.
  b. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
  c. Use `Get-ProvScheme` para obter as informações do seu catálogo de máquinas. Por exemplo:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

  d. Recupere a propriedade personalizada ID do DES do catálogo de máquinas. Por exemplo:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. No Portal do Azure, verifique se o tipo de criptografia do DES associado ao ID do DES é de chaves gerenciadas pela plataforma e gerenciadas pelo cliente.

Determinação do local do arquivo de paginação

O local do arquivo de paginação é determinado de acordo com o seguinte cenário:

Nota:

O local padrão do arquivo de paginação é o disco do SO.

CENÁRIO	LOCAL
A configuração do arquivo de paginação é especificada nas propriedades personalizadas	Conforme especificado nas propriedades personalizadas
Disco de SO efêmero ou hibernação está habilitado	Disco do SO
A VM tem um disco temporário	Disco temporário
MCS IO está habilitado	Disco WBC

Cenários de configuração do arquivo de paginação

A tabela a seguir descreve alguns dos possíveis cenários de configuração do arquivo de paginação durante a preparação da imagem e a atualização do esquema de provisionamento:

DURANTE	CENÁRIO	RESULTADO
Preparação da imagem	Você define o arquivo de paginação da imagem de origem no disco temporário, enquanto o tamanho da VM	O arquivo de paginação é colocado no SO

DURANTE	CENÁRIO	RESULTADO
	que você especifica no esquema de provisionamento não tem disco temporário	
Preparação da imagem	Você define o arquivo de paginação da imagem de origem no disco do SO, enquanto o tamanho da VM que você especifica no esquema de provisionamento tem um disco temporário	O arquivo de paginação é colocado no disco temporário
Preparação da imagem	Você define o arquivo de paginação da imagem de origem no disco temporário e habilita o disco do SO efêmero no esquema de provisionamento	O arquivo de paginação é colocado no disco do SO
Atualização do esquema de provisionamento	Você tenta atualizar o esquema de provisionamento quando a versão do VDA é anterior a 2311	Modifica a configuração do arquivo de paginação com um aviso
Atualização do esquema de provisionamento	Você tenta atualizar o esquema de provisionamento quando a versão do VDA é 2311 ou posterior	Determina o local do arquivo de paginação conforme Determinação do local do arquivo de paginação

Especificar configuração do arquivo de paginação

Usando comandos PowerShell, você pode especificar as configurações do arquivo de paginação, incluindo o local e o tamanho. Isso substitui as configurações do arquivo de paginação determinadas pelo MCS conforme Determinação do local do arquivo de paginação. Você pode fazer isso executando o seguinte comando `New-ProvScheme` durante a criação do catálogo de máquinas.

Considerações importantes

Considere o seguinte antes de prosseguir com a criação do catálogo:

- Você deve fornecer todas as propriedades personalizadas ('PageFileDiskDriveLetterOverride', 'InitialPageFileSizeInMB' e 'MaxPageFileSizeInMB') no comando `New-ProvScheme` ou nenhuma delas.
- Este recurso não é suportado através do Citrix Studio.
- O tamanho inicial do arquivo de paginação deve estar entre 16 MB e 16777216 MB.
- O tamanho máximo do arquivo de paginação deve ser maior ou igual ao tamanho inicial do arquivo de paginação e menor que 16777216 MB.
- Você pode definir o tamanho inicial e o tamanho máximo do arquivo de paginação como zero ao mesmo tempo.

Nota:

Você pode modificar as configurações do arquivo de paginação das VMs recém-adicionadas de um catálogo existente, sem atualizar a imagem mestre. Para modificar as configurações do arquivo de paginação, você precisa da versão 2311 do VDA ou posterior. Você pode modificar as configurações do arquivo de paginação usando os comandos do PowerShell. Para obter mais informações, consulte Modificar configurações do arquivo de paginação.

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "zijinnet" `

-IdentityPoolName "PageFileSettingExample" `

-ProvisioningSchemeName "PageFileSettingExample" `

-InitialBatchSizeHint 1 `

-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-
resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3ef
eea88f.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\zijinnet\
\virtualprivatecloud.folder\\East US.region\\virtualprivatecloud.folder\
\neal-zijincloud-resources.resourcegroup\\neal-zijincloud-resources-
vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\zijinnet\\serviceoffering.folder\
```

```
\Standard_B2ms.serviceoffering" `

-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="d"/> `

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

</CustomProperties>'
```

Modificar configurações do arquivo de paginação

Você pode modificar as configurações do arquivo de paginação das VMs recém-adicionadas a um catálogo existente sem atualizar a imagem mestre. Atualmente, este recurso é aplicável apenas a ambientes Azure.

Para modificar as configurações do arquivo de paginação, você precisa da versão 2311 do VDA ou posterior. Você pode modificar as configurações do arquivo de paginação usando os comandos do PowerShell.

A seguir estão as várias configurações de arquivo de paginação que você pode modificar no ambiente Azure:

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`

- `MaxPageFileSizeInMB`

Modificar as configurações do arquivo de paginação de um catálogo existente

Para modificar as configurações do arquivo de paginação de um catálogo de máquinas existente, execute o comando `Set-ProvScheme`. Neste caso, as atualizações são aplicadas apenas às novas VMs adicionadas ao catálogo. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="StandardSSD_LRS" />

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="D" />

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048" />

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property  xsi:type="StringProperty" Name="Zones" Value="1" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
test-group1" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

Nota:

> Se você habilitar o cache de write-back e tentar definir `PageFileDiskDriveLetterOverride` para `C:` usando o comando PowerShell, o driver de E/S do MCS redireciona automaticamente o arquivo de paginação para uma unidade de disco correta e não `C:`.

Provisionar VMs de catálogo com AMA habilitado

1. Configurar um modelo de perfil de máquina.
   - Se você quiser usar uma VM como modelo de perfil de máquina:
     a. Crie uma VM no portal do Azure.
     b. Ligue a VM.
     c. Adicione a VM à regra de coleta de dados em **Recursos**. Isso invoca a instalação do agente na VM do modelo.

> **Nota:**
>
> Se você precisar criar um catálogo Linux, configure uma máquina Linux.

   - Se você quiser usar a especificação de modelo como um modelo de perfil de máquina:
     a. Configure uma especificação de modelo.
     b. Adicione a seguinte extensão e associação de regra de coleta de dados à especificação de modelo gerada:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",

"apiVersion": "2022-03-01",

"name": "<vm-name>/AzureMonitorWindowsAgent",

"dependsOn": [

    "Microsoft.Compute/virtualMachines/<vm-name>"

],
```

```
"location": "<azure-region>",

"properties": {

    "publisher": "Microsoft.Azure.Monitor",

    "type": "AzureMonitorWindowsAgent",

    "typeHandlerVersion": "1.0",

    "autoUpgradeMinorVersion": true,

    "enableAutomaticUpgrade": true

}

},

 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",

    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"

    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",
```

```
    "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

    }

   }
```

Nota:

Se você tiver uma regra de coleta de dados configurada com um conector de dados do Microsoft Sentinel, você pode simplesmente adicionar `dataCollectionRuleAssociation` na especificação do modelo da mesma forma que uma associação DCR regular. As VMs do catálogo podem então aparecer no DCR do Sentinel e o AMA seria instalado nessas VMs. Para obter informações sobre as melhores práticas para a criação de regras de coleta de dados, consulte Melhores práticas para a criação e gerenciamento de regras de coleta de dados no Azure Monitor.

2. Crie ou atualize um catálogo de máquinas MCS existente.

   - Para criar um novo catálogo MCS:

     a. Selecione essa VM ou especificação de modelo como um perfil de máquina no Studio.

     b. Prossiga com as próximas etapas para criar o catálogo.

   - Para atualizar um catálogo MCS existente, use os seguintes comandos do PowerShell. Neste caso, apenas as novas VMs recebem o modelo de perfil de máquina atualizado.

     ```
     Set-ProvScheme -ProvisioningSchemeName "name"

     -MachineProfile "XDHyp:
     \HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
     machine-profile.vm"
     ```

   - Para atualizar VMs existentes com o modelo de perfil de máquina atualizado, execute `Set-ProvScheme` e, em seguida, execute `Set-ProvVMUpdateTimeWindow`:

```
Set-ProvScheme -ProvisioningSchemeName "name" -MachineProfile
"XDHyp:
\HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
machine-profile.vm"

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

3. Ligue as VMs do catálogo.
4. Vá para o portal do Azure e verifique se a extensão do monitor está instalada na VM e se a VM está aparecendo em Recursos do DCR. Após alguns minutos, os dados de monitoramento são exibidos no Azure Monitor.

Solução de problemas

Para obter informações sobre as diretrizes de solução de problemas para o Azure Monitor Agent, consulte o seguinte:

- `<https://learn.microsoft.com/pt-br/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/>`
- `<https://learn.microsoft.com/pt-br/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/>`

Criar um catálogo usando VMs Spot do Azure

As VMs Spot do Azure permitem que você aproveite a capacidade de computação não utilizada do Azure com uma economia significativa de custos. No entanto, a capacidade de alocar uma VM Spot do Azure depende da capacidade e dos preços atuais. Portanto, o Azure pode despejar sua VM em execução, falhar ao criar a VM ou falhar ao ligar a VM de acordo com a Política de despejo. Portanto, as VMs Spot do Azure são boas para algumas aplicações e desktops não críticos. Para obter mais informações, consulte Usar Máquinas Virtuais Spot do Azure.

Limitações

- Nem todos os tamanhos de VM são suportados para VMs Spot do Azure. Para obter mais informações, consulte Limitações.

  Você pode executar o seguinte comando PowerShell para verificar se um tamanho de VM suporta VMs Spot ou não. Se um tamanho de VM suportar VM Spot, então `SupportsSpotVM` é **True**.

```
(Get-Item "XDHyp:\HostingUnits\azure-res-
conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
AdditionalData
```

- Atualmente, as VMs Spot do Azure não suportam hibernação.

Requisito

Ao criar a origem do perfil da máquina (VM ou especificação de modelo) para o catálogo de VMs Spot do Azure, você deve selecionar Instância Spot do Azure (se estiver usando VM) ou definir `priority` como `Spot` (se estiver usando especificação de modelo).

Etapas para criar um catálogo usando VMs Spot do Azure

1. Crie uma origem de perfil de máquina (VM ou modelo de inicialização).
   - Para criar uma VM usando o portal do Azure, consulte Implantar Máquinas Virtuais Spot do Azure usando o portal do Azure.
   - Para criar uma especificação de modelo, adicione as seguintes propriedades em **resources > type: Microsoft.Compute/virtualMachines > properties** na especificação de modelo. Por exemplo:

```
"priority": "Spot",

"evictionPolicy": "Deallocate",

"billingProfile": {

"maxPrice": 0.01

}
```

Nota:

- A política de remoção pode ser **Deallocate** ou **Delete**.
- Para VMs não persistentes, o MCS sempre define a política de remoção como **Delete**. Se a VM for removida, ela será excluída junto com quaisquer discos não persistentes (por exemplo, disco do SO). Quaisquer discos persistentes (por exemplo, disco de identidade) não são excluídos. No entanto, um disco do SO é

persistente se o tipo de catálogo for persistente ou se a propriedade personalizada `PersistOsDisk` for definida como True. Da mesma forma, um disco WBC é persistente se a propriedade personalizada `PersistWbc` for definida como **True**.

- Para VMs persistentes, o MCS sempre define a política de remoção como Deallocate. Se a VM for removida, ela será desalocada. Nenhuma alteração é feita nos discos.
- O preço máximo é o preço que você está disposto a pagar por hora. Se você estiver usando **Capacity Only**, então este é **-1**. O preço máximo pode ser apenas nulo, -1 ou um decimal maior que zero. Para obter mais informações, consulte Preços.

2. Você pode executar o seguinte comando PowerShell para verificar se um perfil de máquina está habilitado para Azure Spot VM ou não. Se o parâmetro `SpotEnabled` for **True** e `SpotEvictionPolicy` estiver definido como **Deallocate** ou **Delete**, então o perfil de máquina estará habilitado para Azure Spot VM. Por exemplo,

   - Se a origem do perfil da máquina for uma VM, execute o seguinte comando:

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
     delete.vm"). AdditionalData
     ```

   - Se a origem do perfil da máquina for uma especificação de modelo, execute o seguinte comando:

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
     templatespec.templatespec\14.0.0-spot-
     delete.templatespecversion").AdditionalData
     ```

3. Crie um catálogo de máquinas usando um perfil de máquina com o comando PowerShell `New-ProvScheme`.

Você pode atualizar um catálogo usando o comando `Set-ProvScheme`. Você também pode atualizar VMs existentes usando o comando PowerShell `Set-ProvVmUpdateTimeWindow`. O perfil da máquina é atualizado no próximo ligar.

Remoções em uma VM Spot do Azure em execução

Se a capacidade de computação estiver indisponível ou o preço por hora for superior ao preço máximo configurado, o Azure removerá uma VM Spot em execução. Por padrão, você não é notificado de uma remoção. A VM simplesmente congela e é removida. A Microsoft recomenda usar Eventos Agendados para monitorar remoções. Consulte Monitorar continuamente para remoção. Você também pode executar scripts de dentro de uma VM para receber uma notificação antes da remoção. Por exemplo, a Microsoft tem um script de sondagem em Python ScheduledEvents.cs.

Solução de problemas

- Você pode ver as propriedades da VM Spot em customMachineData da VM provisionada usando o comando `Get-ProvVM`. Se o campo de prioridade estiver definido como **Spot**, então o Spot está em uso.
- Você pode verificar se uma VM está usando Spot no Portal do Azure:

  a. Encontre a VM no Portal do Azure.

  b. Vá para a página **Visão geral**.

  c. Role para baixo até o final e localize a seção **Azure Spot**.

    - Se o Spot não estiver em uso, este campo estará vazio.
    - Se o Spot estiver em uso, os campos **Azure Spot** e **Política de remoção do Azure Spot** estarão definidos.

1. Você pode verificar o perfil de faturamento ou o preço máximo por hora para a VM na página de Configuração.

Configurar tamanhos de VM de backup

Nuvens públicas podem ficar sem capacidade para um tamanho de VM específico. Quando o Azure não tem capacidade, o MCS recorre a uma lista pré-configurada de tamanhos de VM de backup. Esta lista selecionada, adaptada pelo cliente às suas necessidades de carga de trabalho, aumenta a probabilidade de que um desses tamanhos tenha capacidade suficiente para inicializar no Power On ou Resume se a VM foi hibernada anteriormente.

Quando uma ação de energia é iniciada, o MCS implementa uma sequência de fallback automatizada para garantir alta disponibilidade. O fluxo de trabalho é o seguinte:

1. Iniciação: Um usuário ou administrador emite um comando de **PowerOn** ou **Resume** via Web Studio.

2. Monitoramento de Exceções: O MCS tenta iniciar a VM usando a configuração primária. Ele monitora exceções específicas de capacidade do Azure, como Quota Exceeded, Allocation Failed ou Zonal Allocation Failed e SKU Not Available (Podemos generalizar isso e dizer que monitoramos o Azure para quaisquer falhas de capacidade ou alocação)
3. Fallback Sequencial: Se um dos erros acima ocorrer, o MCS itera automaticamente pela lista BackupVmConfiguration sequencialmente até que a VM inicie com sucesso. Se todos os tamanhos na BackupVmConfiguration falharem, a ação de energia é marcada como falha.
4. Lógica de Atualização vs. Recriação:
    - Atualização Direta: Na maioria dos casos, o MCS realiza uma simples atualização do tamanho da VM para o SKU de backup e, em seguida, liga a VM.
    - Excluir e Recriar: Para manter a integridade do ambiente, certas transições exigem que a VM existente seja excluída e uma nova seja criada em seu lugar. Isso ocorre quando:
        - Alternando entre tipos de VM Spot e Regular.
        - Alternando entre tamanhos de VM com suporte a Disco de Recurso (Armazenamento Temporário) e aqueles sem.
5. Persistência e Recuperação de Dados: Durante uma operação de "Excluir e Recriar", se todos os tamanhos de backup também falharem devido a escassez extrema de capacidade do Azure, a VM pode desaparecer temporariamente do Portal do Azure. No entanto, nenhuma perda de dados ocorre. Na próxima tentativa de PowerOn, o MCS recriará a VM usando as configurações originais e anexará novamente os discos de SO, Identidade e Dados existentes.
6. Faturamento de VM Spot e Comportamento de MaxPrice Se sua configuração primária utiliza um Perfil de Máquina (Modelo de VM) com prioridade Spot e um Perfil de Faturamento específico (MaxPrice), a seguinte lógica se aplica durante o fallback:
    - Tamanho Primário: Usa o MaxPrice definido em seu Perfil de Máquina. A remoção é baseada em Preço ou Capacidade.
    - Tamanhos Spot de Backup: A propriedade BackupVmConfiguration atualmente não oferece suporte a uma entrada `MaxPrice` exclusiva para cada SKU, o MCS lida com a transição da seguinte forma:
    - Redefinição de MaxPrice: O MCS define o MaxPrice como -1.
    - Mudança na Política de Despejo: Isso altera o comportamento de despejo do Azure de baseado em preço para baseado em capacidade.

- Preços: Você será cobrado pelo preço Spot atual, limitado à taxa padrão Pay-As-You-Go (PAYG) para aquela SKU de backup. Isso garante que a VM seja despejada apenas se o Azure realmente ficar sem capacidade física, em vez de devido a uma flutuação de preço.

7. Persistência do Estado de Backup: Uma vez iniciada, a VM permanece no tamanho de backup durante a sessão até que uma solicitação de Desligamento ou Hibernação seja processada.
8. Restauração do Tamanho Primário: Na próxima inicialização ou retomada, o MCS sempre tenta "retornar" a VM à sua Oferta de Serviço Primária (conforme definido no Catálogo ou Perfil da Máquina). Se o tamanho primário permanecer indisponível, a sequência de fallback se repete.

Desafios com a hibernação

O Azure não permite alterações de tamanho em uma VM hibernada, conforme explicado em Limitações gerais. A VM deve estar no estado Parado. Portanto, antes de alterar o tamanho, o MCS emite uma solicitação de Desalocação para limpar o estado hibernado, o que faz com que o estado de hibernação da VM seja perdido. O MCS então percorre os tamanhos de backup, atualiza o tamanho da VM e a liga.

Cenários não suportados para o tamanho da VM de backup

As seguintes configurações não são suportadas:

- Para VMs persistentes, os seguintes cenários não são suportados:
  - A VM usa DiskControllerType SCSI, mas o tamanho da VM de backup suporta apenas DiskControllerType NVMe.
  - A VM usa DiskControllerType NVMe, mas o tamanho da VM de backup suporta apenas DiskControllerType SCSI.
- Para VMs não persistentes com MCSIO ativado, a mudança para um tamanho sem armazenamento temporário não é suportada se o disco de cache de write-back usar armazenamento temporário de Disco de Recurso.

Pré-requisitos para configurar tamanhos de VM de backup

Se alguma das seguintes condições não for atendida, um erro será gerado.

- Suportado apenas quando o Perfil da Máquina está em uso no Catálogo de Máquinas.
- O tipo é opcional e pode ser Spot ou Regular. O padrão é Regular se não especificado.
- Cada combinação de ServiceOffering deve ser única para evitar configurações repetidas.
- A Cota Regional deve ter núcleos suficientes para o ServiceOffering.

- A contagem de interfaces de rede não deve exceder o máximo permitido para um ServiceOffering.
- Os ServiceOfferings nesta lista de BackupVmConfiguration devem ser compatíveis com as Propriedades Personalizadas atuais, as capacidades da Imagem Mestra e o MachineProfile. Alguns cenários de falha são:
  - Hosts Dedicados do Azure: Os hosts no Grupo de Hosts devem suportar o ServiceOffering se hosts dedicados forem usados.
  - Disco de SO Efêmero: O ServiceOffering deve suportar Discos de SO Efêmeros se ativado nas propriedades personalizadas.
  - Armazenamento Premium: O ServiceOffering deve suportar armazenamento Premium se especificado nas propriedades personalizadas.
  - Rede Acelerada: O ServiceOffering deve suportar Rede Acelerada se estiver ativada no MachineProfile.
  - DiskEncryptionAtHost: O ServiceOffering deve suportar Criptografia no Host se ativada no MachineProfile.
  - Armazenamento Temporário: Se o MCSIO estiver em uso e o Cache de Gravação estiver no disco Temporário, o uso de um tamanho de VM que não possui Armazenamento Temporário não é permitido.
  - HyperVGeneration: O ServiceOffering deve ser compatível com a geração de VM (1 ou 2) especificada em MasterImageVM.
  - TrustedLaunch: O ServiceOffering deve suportar TrustedLaunch se ativado no MachineProfile.
  - VMs Confidenciais: ServiceOffering deve suportar VM Confidencial se ativado em MachineProfile.

Criar um catálogo com tamanhos de VM de backup

> **Nota:**

> Para resolver o problema de congelamento da interface do usuário do Studio, substitua todas as aspas simples por `"` ao executar os comandos do PowerShell.

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.

3. Crie um catálogo de Broker. Este catálogo é preenchido com máquinas que estão prestes a ser criadas.
4. Crie um pool de identidades. Isso se torna um contêiner para as contas AD criadas para as máquinas que serão criadas.
5. Crie um esquema de provisionamento com o perfil da máquina. Consulte Como configurar a configuração de backup.
6. Atualize o `BrokerCatalog` com o ID exclusivo do esquema de provisionamento.
7. Crie e adicione VMs ao catálogo.

Atualizar um catálogo existente

Você pode atualizar um esquema de provisionamento usando o comando `Set-ProvScheme`. Consulte Como configurar a configuração de backup.

Atualizar VMs existentes

Você pode atualizar VMs existentes em um catálogo usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`. O comando atualiza as VMs criadas a partir do esquema de provisionamento associado ao catálogo no próximo ligar dentro da janela de tempo fornecida. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
```

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

Você pode configurar a lista de tamanhos de VM de backup para um número selecionado de VMs MCS existentes usando o comando `Set-ProvVM`. No entanto, para aplicar as atualizações, defina uma janela de tempo de atualização para as VMs usando `Set-ProvVMUpdateTimeWindow` e inicie as VMs dentro da janela. Por exemplo,

1. Execute o comando `Set-ProvVM` para configurar a lista de tamanhos de VM de backup para uma VM MCS existente selecionada. Por exemplo:

   ```
   Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

   -CustomProperties
   ```

```
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
Name=`"BackupVmConfiguration`" Value=`"[{&quot;ServiceOffering&quot;:
&quot;Standard_D2as_v4&quot;, &quot;Type&quot;: &quot;Spot&quot;},
{&quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;,
&quot;Type&quot;: &quot;Regular&quot;}, {&quot;ServiceOffering&quot;:
&quot;Standard_D2s_v3&quot;, &quot;Type&quot;: &quot;Spot&quot;}]`"/>
</CustomProperties>"
```

2. Execute o comando `Set-ProvVMUpdateTimeWindow` para aplicar as atualizações. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

Copiar tags em todos os recursos

Você pode copiar tags especificadas em um perfil de máquina para todos os recursos, como várias NICs e discos (disco do SO, disco de identidade e disco de cache de write-back) de uma nova VM ou de uma VM existente em um catálogo de máquinas. A origem do perfil da máquina pode ser uma VM ou uma especificação de modelo ARM.

Nota:

> Você deve adicionar a política nas tags (consulte Atribuir definições de política para conformidade de tags) ou adicionar as tags em uma origem de perfil de máquina para reter as tags nos recursos.

Pré-requisitos

Crie a origem do perfil da máquina (VM ou especificação de modelo ARM) para ter tags na VM, discos e NICs dessa VM.

- Se você deseja ter uma VM como entrada de perfil de máquina, aplique tags na VM e em todos os recursos no portal do Azure. Consulte Aplicar tags com o portal do Azure.
- Se você deseja ter uma especificação de modelo ARM como entrada de perfil de máquina, adicione o seguinte bloco de tags em cada recurso.

```
 "tags": {

"TagC": "Value3"

},
```

> **Nota:**
>
> Você pode ter no máximo um disco e pelo menos uma NIC na especificação do modelo.

Copiar tags para os recursos de uma VM em um novo catálogo de máquinas

1. Crie um catálogo não persistente ou persistente com uma VM ou especificação de modelo ARM como entrada de perfil de máquina.
2. Adicione uma VM ao catálogo e ligue-a. Você deve ver as tags especificadas no perfil da máquina copiadas para os recursos correspondentes dessa VM.

> **Nota:**
>
> Você receberá um erro se houver uma incompatibilidade no número de NICs fornecidas no perfil da máquina e no número de NICs que você deseja que as VMs usem.

Modificar tags nos recursos de uma VM existente

1. Crie um perfil de máquina com as tags em todos os recursos.
2. Atualize o catálogo de máquinas existente com o perfil de máquina atualizado. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. Desligue a VM na qual você deseja aplicar as atualizações.
4. Solicite uma atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. Ligue a VM.
6. Você deve ver as tags especificadas no perfil da máquina copiadas para os recursos correspondentes.

Nota:

Você receberá um erro se houver uma incompatibilidade no número de NICs fornecidas no perfil da máquina e no número de NICs fornecidas no `Set-ProvScheme`.

Criar um catálogo de discos WBC pré-formatados

Você pode criar um catálogo de discos WBC pré-formatados para melhorar o desempenho de inicialização das máquinas provisionadas. Para implementar essa funcionalidade, crie um catálogo do Azure com o WBC ativado e inclua uma propriedade personalizada adicional `PreformatWriteBackCache` como `True`.

Você pode atualizar um catálogo existente usando o comando `Set-ProvScheme` para atualizar o tamanho do disco WBC.

Este recurso é compatível com o fluxo de trabalho de gerenciamento de imagem onde o MCS separa a fase de masterização do fluxo de trabalho geral de provisionamento. Para obter informações sobre gerenciamento de imagem, consulte Gerenciamento de imagem.

Exemplo de criação de um catálogo do Azure com WBC habilitado e `PreformatWriteBackCache` como `True`:

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `

-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

Exemplo de atualização do tamanho do cache de disco WBC de um catálogo existente:

```
Set-ProvScheme -ProvisioningSchemeName provisioningschemename
-WriteBackCacheDiskSize 127
```

Excluir disco WBC no desligamento para catálogos Citrix Provisioning™ provisionados por MCS

Ao criar catálogos Citrix Provisioning provisionados por MCS no Azure, você pode provisionar o disco WBC para ser não persistente (`PersistWBC` como False). Essa configuração ajuda a excluir o disco de cache de gravação (WBC) depois de desligar a VM para catálogos Citrix Provisioning provisionados por MCS no Azure.

Condição:

Você deve definir a propriedade personalizada `PreformatWriteBackCache` como `True` para que este recurso funcione.

Exemplo de criação de um catálogo do Azure com `PersistWBC` como `False` e `PreformatWriteBackCache` como `True`:

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `
```

```
-CustomProperties $customProperties `

-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

Você também pode atualizar um catálogo existente usando o comando `Set-ProvScheme` para atualizar a propriedade personalizada `PersistWBC`.

Provisionar disco de dados

Você pode criar e atribuir um disco de dados persistente a uma VM persistente ou não persistente criada por MCS de um catálogo de máquinas MCS no Azure.

O disco de dados deve ser provisionado a partir de um disco gerenciado como uma fonte de imagem.

Propriedades do disco de dados

O disco de dados deriva propriedades de propriedades personalizadas ou do modelo de disco do SO se as propriedades não forem especificadas nas propriedades personalizadas.

- Propriedades derivadas de propriedades personalizadas
  - `DiskEncryptionSetId`
  - `Zones`
  - `StorageType`
- Propriedades derivadas do modelo de disco do SO se não especificadas nas propriedades personalizadas
  - `DiskEncryptionSetId`
  - `Zones`
  - `StorageType`

> **Nota:**

- Se o Armazenamento Redundante de Zona (ZRS) não for especificado nas propriedades personalizadas ou no modelo de disco do SO, o disco de dados será colocado na mesma zona que o disco do SO e o disco de Identidade.
- As tags são derivadas apenas do modelo de disco do SO.

Limitações

As seguintes operações não são atualmente suportadas:

- Provisionamento de mais de um disco de dados.
- Provisionamento de discos de dados não persistentes.
- Criação de um disco de dados com um modelo.
- Modificar catálogos e VMs existentes para usar discos de dados.
- Redefinir o disco de dados.
- Atualização da imagem do disco de dados.
- Usar uma fonte diferente de um disco gerenciado.
- Armazenar disco de dados na Galeria de Computação do Azure (ACG).
- Usar `StorageTypeAtShutdown` para o disco de dados

Criar um catálogo com disco de dados

Inclua os seguintes parâmetros no comando PowerShell `New-ProvScheme` para provisionar um catálogo de máquinas MCS com disco de dados.

- `DataDisk`: Caminho para um item de inventário do tipo ManagedDisk válido.
- `DataDiskPersistence`: Para indicar se o `DataDisk` é persistente ou não persistente. No entanto, atualmente, apenas discos de dados persistentes são suportados.

Por exemplo:

```
New-ProvScheme  -CleanOnBoot -HostingUnitName "<HostingUnitName >"
-IdentityPoolName "<IdentityPoolName >" -InitialBatchSizeHint 1
-MasterImageVM disk.manageddisk -NetworkMapping <NetworkMapping >
-ProvisioningSchemeName "<ProvisioningSchemeName >" -DataDisk "XDHyp:
\HostingUnits\Azure-Resources-1\image.folder\<resourcegroupname>\xxxx-
datadisk.manageddisk"  -DataDiskPersistence "Persistent"  -Scope @()
```

```
-VMCpuCount 4  -VMMemoryMB 6144  -TenancyType Shared  -FunctionalLevel
"L7_20"
```

Determinar se um disco de dados está em uso

Faça o seguinte para verificar se o disco de dados está atribuído a uma VM:

- Execute `Get-ProvVm` e verifique o `CustomVmData` da VM. Se a VM estiver usando o disco de dados, haverá um registro de disco com a função `DiskRole.DataDisk`.
- Verifique se um disco de dados está presente na VM no portal do Azure.

Excluir um disco de dados

Se você excluir o catálogo, o disco de dados será excluído, a menos que você use a opção `forgetVM` ou `purgeDBOnly`. Se você excluir a VM, o disco de dados será excluído, a menos que você use a opção `forgetVM` ou `purgeDBOnly`.

Migrar de discos não gerenciados para gerenciados

Em September 30, 2025, o Azure desativará oficialmente os discos não gerenciados (ou seja, VHDs). Quaisquer VMs existentes que usam discos não gerenciados serão interrompidas e desalocadas após o prazo.

No entanto, você pode migrar suas VMs provisionadas pelo MCS de discos não gerenciados para discos gerenciados, o que ajuda a evitar interrupções de serviço devido aos planos de desativação de discos não gerenciados do Azure.

Todos os discos não gerenciados anexados à VM são convertidos. Isso inclui o Disco de Identidade, o Disco do SO e o Disco WBC (se usado).

Para obter mais informações sobre o plano de desativação de discos não gerenciados do Azure, consulte Migre seus discos não gerenciados do Azure até September 30, 2025.

Casos de uso

Este recurso se aplica a catálogos provisionados pelo MCS persistentes e não persistentes.

Ele também oferece suporte à migração para VMs sob demanda e não sob demanda (legadas):

- VMs sob demanda: Transfira seus discos existentes de não gerenciados para gerenciados para se alinhar ao suporte atualizado do Azure.
- VMs não sob demanda (legadas): VMs legadas ou não sob demanda suportam apenas discos não gerenciados. Use este recurso para converter suas VMs legadas em sob demanda, migrando também para discos gerenciados.

Para obter mais informações sobre o provisionamento sob demanda, consulte Provisionamento sob demanda do Azure.

Limitações

- Depois que um catálogo de máquinas ou VM é convertido para discos gerenciados, ele não pode ser convertido de volta para discos não gerenciados
- Para VMs não sob demanda (legadas), o processo de migração inclui convertê-las para provisionamento sob demanda. Você não pode converter apenas os discos e continuar a usar VMs não sob demanda.

Considerações importantes

- A conversão não ocorre automaticamente. Ela acontece como parte de uma operação de inicialização.
- Se várias atualizações forem solicitadas para uma VM, a conversão do disco terá precedência. Atualizações adicionais são adiadas até uma inicialização subsequente.
- Depois que a VM é convertida e inicializada com sucesso, os VHDs da VM são limpos para economizar custos. A própria conta de armazenamento não é limpa.
    - Um disco base ainda pode existir na conta de armazenamento. Você pode executar uma atualização de catálogo, e um novo disco base de snapshot (ou ACG) é criado.
    - Depois que todas as VMs no catálogo são convertidas e o novo disco base é criado, a conta de armazenamento vazia pode ser excluída.

Permissões necessárias

Você precisa da seguinte permissão em seu Azure Service Principal para permitir a conversão de discos não gerenciados para gerenciados:

```
Microsoft.Compute/virtualMachines/convertToManagedDisks/write
```

Etapas de configuração

Para Catálogos Sob Demanda:

1. Execute `Set-ProvScheme` (ou `Set-ProvVM` para VMs persistentes) para atualizar `UseManagedDisks` para `True`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "<provscheme-name>"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"UseManagedDisks`" Value=`"true`" /></CustomProperties>"
```

```
Set-ProvVM -ProvisioningSchemeName "<provscheme-name>" -VMName "<vm-
name>" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /
></CustomProperties>"
```

2. Execute `Set-ProvVMUpdateTimeWindo`w` para aplicar as atualizações. Neste exemplo, a atualização é aplicada na próxima inicialização da VM.

```
Set-ProvVmUpdateTimeWindow -ProvisioningSchemeName "<provscheme-name>"
-VMName "<vm-name>"
```

3. Ligue as VMs.

Para Catálogos Não Sob Demanda (Legados):

1. Executar `Set-ProvScheme` (ou `Set-ProvVM` para VMs persistentes) para configurar `Set DeploymentSchema` para `1.1`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "<provscheme-name>"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"DeploymentSchema`" Value=`"1.1`" /></CustomProperties>"
```

```
Set-ProvVM -ProvisioningSchemeName "<provscheme-name>" -VMName "<vm-
name>" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"DeploymentSchema`" Value=`"1.1`" /
></CustomProperties>
```

2. Execute `Set-ProvVMUpdateTimeWindow` para aplicar as atualizações. Neste exemplo, a atualização é aplicada no próximo ligar da VM.

```
Set-ProvVmUpdateTimeWindow -ProvisioningSchemeName "<provscheme-name>"
-VMName "<vm-name>"
```

3. Ligue as VMs.

Solução de problemas

Se uma VM falhar ao converter de discos não gerenciados para gerenciados:

- Verifique se as propriedades personalizadas `UseManagedDisks` ou `DeploymentSchema` estão definidas corretamente:
  - Se estiver usando `Set-ProvScheme`, verifique as propriedades personalizadas do ProvScheme executando `Get-ProvScheme`. Para obter mais informações, consulte Get-ProvScheme.
  - Se estiver usando `Set-ProvVM`, verifique se a VM tem uma nova configuração com a propriedade personalizada atualizada executando `Get-ProvVMConfiguration`. Para obter mais informações, consulte Set-ProvVM.
- Verifique se a seguinte permissão está presente no seu Azure Service Principal:
  - `Microsoft.Compute/virtualMachines/convertToManagedDisks/write`
- Execute `Get-ProvOperationEvent` para visualizar quaisquer avisos para o Esquema de Provisionamento. Para obter mais informações, consulte Get-ProvOperationEvent. Por exemplo:

```
Get-ProvOperationEvent -LinkedObjectType ProvisioningScheme
-LinkedObjectUid <your-provscheme-id>
```

Onde ir em seguida

- Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.
- Para revisar todo o processo de configuração, consulte Planejar e construir uma implantação.
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Microsoft Azure.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o Microsoft Azure Resource Manager
- Criar catálogos de máquinas

Criar um catálogo do Microsoft SCVMM

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização do Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Antes de criar um catálogo VMM, você precisa concluir a criação de uma conexão com o VMM. Consulte Conexão com o Microsoft System Center Virtual Machine Manager.

Criar uma VM mestre

- Instale um VDA na VM mestre e selecione a opção para otimizar a área de trabalho. Isso melhora o desempenho.
- Tire um instantâneo da VM mestre para usar como backup.
- Crie áreas de trabalho virtuais.

MCS em compartilhamentos de arquivos SMB 3

Para catálogos de máquinas criados com MCS em compartilhamentos de arquivos SMB 3 para armazenamento de VM, as credenciais devem atender aos seguintes requisitos para garantir que as chamadas da XenServer® Communications Library (HCL) se conectem com sucesso ao armazenamento SMB.

- As credenciais de usuário do VMM devem incluir acesso total de leitura e gravação ao armazenamento SMB.
- As operações de disco virtual de armazenamento durante eventos do ciclo de vida da VM são realizadas através do servidor Hyper-V usando as credenciais de usuário do VMM.

Para obter mais informações sobre SMB 3, consulte Visão geral do compartilhamento de arquivos usando o protocolo SMB 3 no Windows Server.

Ao usar o VMM 2012 SP1 com Hyper-V no Windows Server 2012: Ao usar SMB como armazenamento, habilite o Authentication Credential Security Support Provider (CredSSP) do Cloud Connector para máquinas Hyper-V individuais. Para obter mais informações, consulte CTX137465.

Usando uma sessão remota padrão do PowerShell V3, o HCL no Cloud Connector usa o CredSSP para abrir uma conexão com a máquina Hyper-V. Esse recurso passa credenciais de usuário criptografadas com Kerberos para a máquina Hyper-V, e os comandos do PowerShell na sessão na máquina Hyper-V remota são executados com as credenciais fornecidas (neste caso, as do usuário VMM), para que os comandos de comunicação para o armazenamento funcionem corretamente.

As tarefas a seguir usam scripts PowerShell que se originam no HCL. Os scripts são então enviados para a máquina Hyper-V para atuar no armazenamento SMB 3.0.

Consolidar Imagem Mestra: Uma imagem cria um novo esquema de provisionamento MCS (catálogo de máquinas). Ela clona e nivela a VM mestra, pronta para criar novas VMs a partir do novo disco criado (e remove a dependência da VM mestra original).

ConvertVirtualHardDisk no namespace root\\virtualization\\v2

Exemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

Criar disco de diferenciação: Cria um disco de diferenciação a partir da imagem gerada pela consolidação da imagem. O disco de diferenciação é então anexado a uma nova VM.

CreateVirtualHardDisk no namespace root\\virtualization\\v2

Exemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);
```

```
$result
```

Carregar discos de identidade: O HCL não pode carregar diretamente o disco de identidade para o armazenamento SMB. Portanto, a máquina Hyper-V deve carregar e copiar o disco de identidade para o armazenamento. Como a máquina Hyper-V não pode ler o disco do Cloud Connector, o HCL deve primeiro copiar o disco de identidade através da máquina Hyper-V da seguinte forma.

1. O HCL carrega a Identidade para a máquina Hyper-V através do compartilhamento do administrador.
2. A máquina Hyper-V copia o disco para o armazenamento SMB através de um script PowerShell executado na sessão remota do PowerShell.

   Uma pasta é criada na máquina Hyper-V e as permissões dessa pasta são bloqueadas apenas para o usuário VMM (através da conexão remota do PowerShell).
3. O HCL exclui o arquivo do compartilhamento do administrador.
4. Quando o HCL conclui o upload do disco de identidade para a máquina Hyper-V, a sessão remota do PowerShell copia os discos de identidade para o armazenamento SMB e, em seguida, os exclui da máquina Hyper-V.

A pasta do disco de identidade é recriada se for excluída para torná-la disponível para reutilização.

Baixar discos de identidade: Assim como nos uploads, os discos de identidade passam pela máquina Hyper-V para o HCL. O processo a seguir cria uma pasta que tem permissões de usuário VMM apenas no servidor Hyper-V, caso ela não exista.

1. A máquina HyperV copia o disco do armazenamento SMB para o armazenamento local do Hyper-V usando um script PowerShell executado na sessão remota do PowerShell V3.
2. O HCL lê o disco do compartilhamento do administrador da máquina Hyper-V para a memória.
3. O HCL exclui o arquivo do compartilhamento do administrador.

Criar catálogo com um perfil de máquina

Você pode usar um perfil de máquina para criar e atualizar um catálogo de máquinas MCS em ambientes do System Center Virtual Machine Manager (SCVMM). Você pode habilitar o vTPM. Você também pode adicionar tags personalizadas de uma VM de perfil de máquina às VMs provisionadas.

Considerações importantes

- A imagem mestre só pode ser um instantâneo e não uma VM.
- Você só pode usar a VM como a origem do perfil de máquina.
- Em ambientes do System Center Virtual Machine Manager (SCVMM), você pode usar um perfil de máquina para criar e atualizar um catálogo de máquinas MCS. Você pode habilitar o vTPM e/ou o Secure Boot. Você também pode adicionar tags personalizadas de uma VM de perfil de máquina às VMs provisionadas.
- Se a imagem mestre tiver o vTPM habilitado, você deverá habilitar o vTPM na origem do perfil de máquina.
- O vTPM é suportado apenas em máquinas de Geração 2.
- Os seguintes parâmetros sobrescrevem os valores capturados em um perfil de máquina se fornecidos separadamente:
  - VMCpuCount
  - VMMemoryMB
  - Armazenamento em disco
- As tags personalizadas são herdadas apenas do perfil da máquina e não da imagem mestre. A tag `CitrixProvisioningSchemeId` é adicionada por padrão à VM. Se você não quiser incluir a tag `CitrixProvisioningSchemeId`, adicione o parâmetro `-NoVmTagging` ao criar uma unidade de hospedagem. Exemplo:

```
New-Item -HypervisorConnectionName  $ConnectionName `

-NetworkPath @($NetworkPath) `

-Path @($HostingUnitPath) `

-PersonalvDiskStoragePath @() `

-RootPath $RootPath `

-StoragePath @($StoragePath) `

-NoVmTagging
```

- Você pode atualizar um catálogo existente usando o comando `Set-ProvScheme`.

MATRIZ DE SUPORTE

IMAGEM MESTRE	PERFIL DA MÁQUINA	RESULTADO
Sem vTPM	vTPM	Máquinas clonadas têm vTPM habilitado
vTPM	vTPM	Máquinas clonadas têm vTPM habilitado
vTPM	Sem vTPM	Erro de pré-verificação - operação bloqueada
Sem vTPM	Sem vTPM	Máquinas clonadas não têm vTPM

Criar um catálogo de máquinas usando um perfil de máquina

1. Crie uma VM para ser uma fonte de perfil de máquina. Para obter mais informações, consulte Provisionar máquinas virtuais na malha VMM. Você não pode alterar a **Geração** depois de selecionada. Você pode fazer o seguinte no SCVMM:
   - Para habilitar o vTPM:
     a. Depois de criar a VM, faça login no host Hyper-V e encontre sua VM em **Gerenciador do Hyper-V**.
     b. Clique com o botão direito do mouse na VM e vá para **Configurações**.
     c. Em **Segurança**, selecione a caixa de seleção **Habilitar Módulo de Plataforma Confiável**.
2. Abra uma janela do **PowerShell**.
3. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
4. Crie um catálogo de Broker. Este catálogo é preenchido com máquinas que estão prestes a ser criadas.
5. Crie um pool de identidades. Isso se torna um contêiner para as contas AD criadas para as máquinas que serão criadas.
6. Crie um esquema de provisionamento com o perfil da máquina. Por exemplo:

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. Atualiza o catálogo do Broker com o ID exclusivo do esquema de provisionamento.
8. Crie e adicione VMs ao catálogo.

Atualizar um catálogo existente

Você pode atualizar um catálogo existente usando o comando Set-ProvScheme. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

Remover uma VM

Você pode optar por remover uma VM de um catálogo, mas não excluir a VM do SCVMM. Neste caso, a tag `CitrixProvisioningSchemeId` é removida apenas da VM. As tags personalizadas não são excluídas da VM. Você pode remover uma VM usando o Studio ou comandos PowerShell.

REMOVER UMA VM USANDO O STUDIO

1. Selecione e clique com o botão direito na VM.
2. Clique em **Excluir**.
3. Selecione **Remover as máquinas virtuais do catálogo, mas não excluir as máquinas virtuais**.

USANDO COMANDOS POWERSHELL

`Remove-ProvVM` com o parâmetro `ForgetVM`. Para obter mais informações, consulte:

- Remover tags
- Excluir máquinas sem acesso ao hypervisor

Onde ir a seguir

- Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.

- Para revisar todo o processo de configuração, consulte Planejar e construir uma implantação.
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Microsoft System Center Virtual Machine Manager.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o Microsoft System Center Virtual Machine Manager
- Criar catálogos de máquinas

Criar um catálogo Nutanix

(/pt-br/citrix-daas/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização Nutanix.

> **Nota:**
>
> Antes de criar um catálogo Nutanix, você precisa concluir a criação de uma conexão com o Nutanix. Consulte Conexão com Nutanix.

Criar um catálogo de máquinas usando a versão do modelo de máquina Nutanix

Ao criar um catálogo de máquinas provisionado por MCS com uma conexão de host Nutanix AHV Prism Central gerenciada pela Citrix, a imagem base é criada a partir de uma versão de modelo de VM Nutanix. Uma vantagem fundamental é que o Nutanix Prism Central permite que um modelo de VM seja usado em vários clusters. Como resultado, os administradores Citrix podem usar uma única versão de modelo de VM Nutanix como a VM mestre para vários catálogos de máquinas MCS, mesmo que esses catálogos estejam em clusters Nutanix diferentes.

Antes de criar o catálogo, crie uma VM mestre e converta-a em uma versão de modelo de VM no Nutanix Prism Central. Consulte a documentação do Nutanix para obter as etapas.

Você pode criar um catálogo usando:

- Studio. Você também pode criar um catálogo usando VMs existentes. Consulte Criar um catálogo de máquinas usando máquinas existentes (gerenciadas por energia)
- Comandos PowerShell

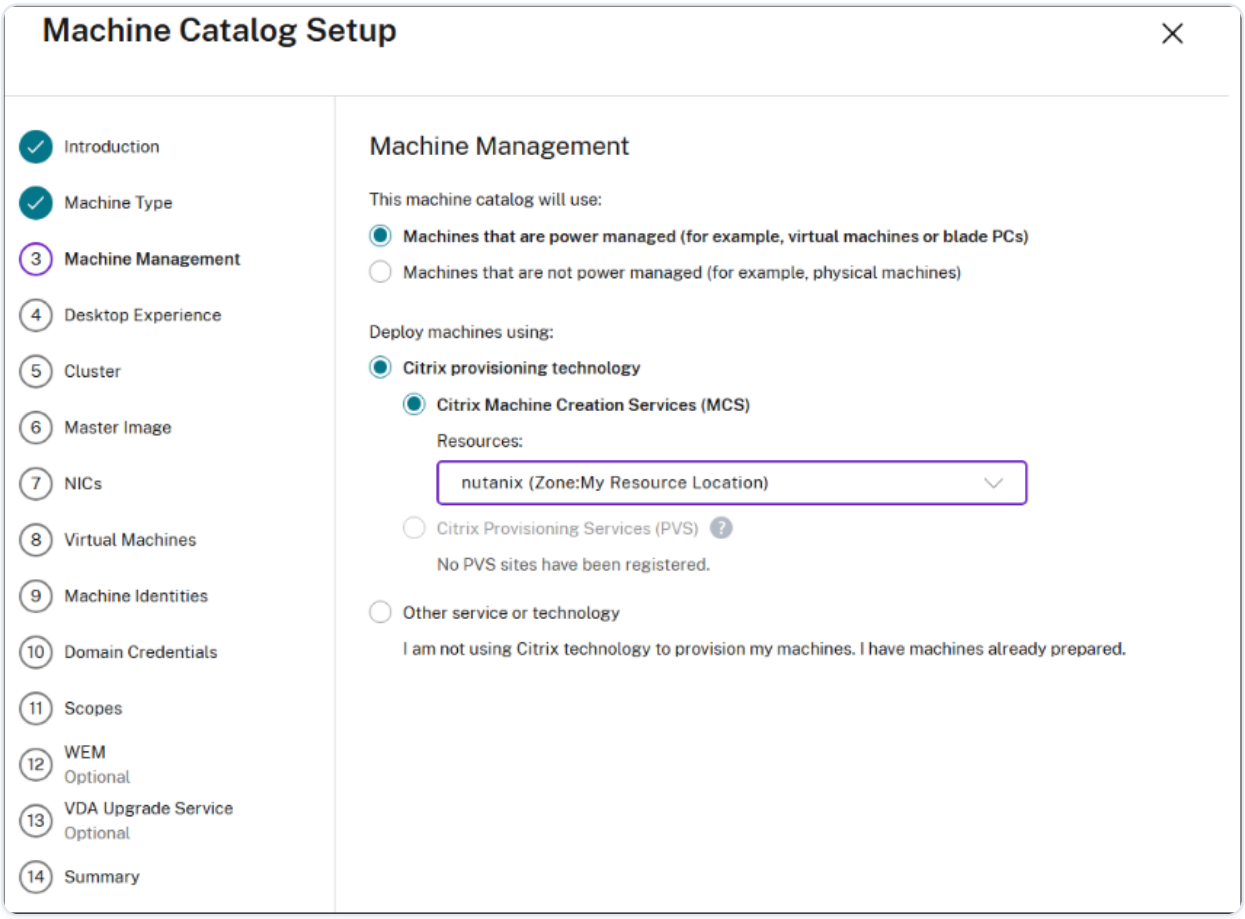
Limitações

- Não há suporte para anexar várias NICs à mesma sub-rede.
- Devido à limitação do Nutanix, cada catálogo de máquinas provisionado por MCS só pode ser atribuído com NICs em um único tipo de rede entre redes Overlay, sub-redes básicas VLAN e sub-redes VLAN.
- Em alguns cenários, a atualização da imagem mestre do MCS para um catálogo de máquinas não persistente pode causar problemas potenciais. Consulte Inicialização Segura e vTPM no Nutanix Prism Central.
- Ao criar um catálogo de máquinas no Nutanix, o nome do cluster que contém um ponto (.) não é suportado.
- Ao selecionar um modelo de VM Nutanix como imagem mestre, o nome do modelo ou o nome da versão do modelo não deve conter caracteres como **#** ou **&**.

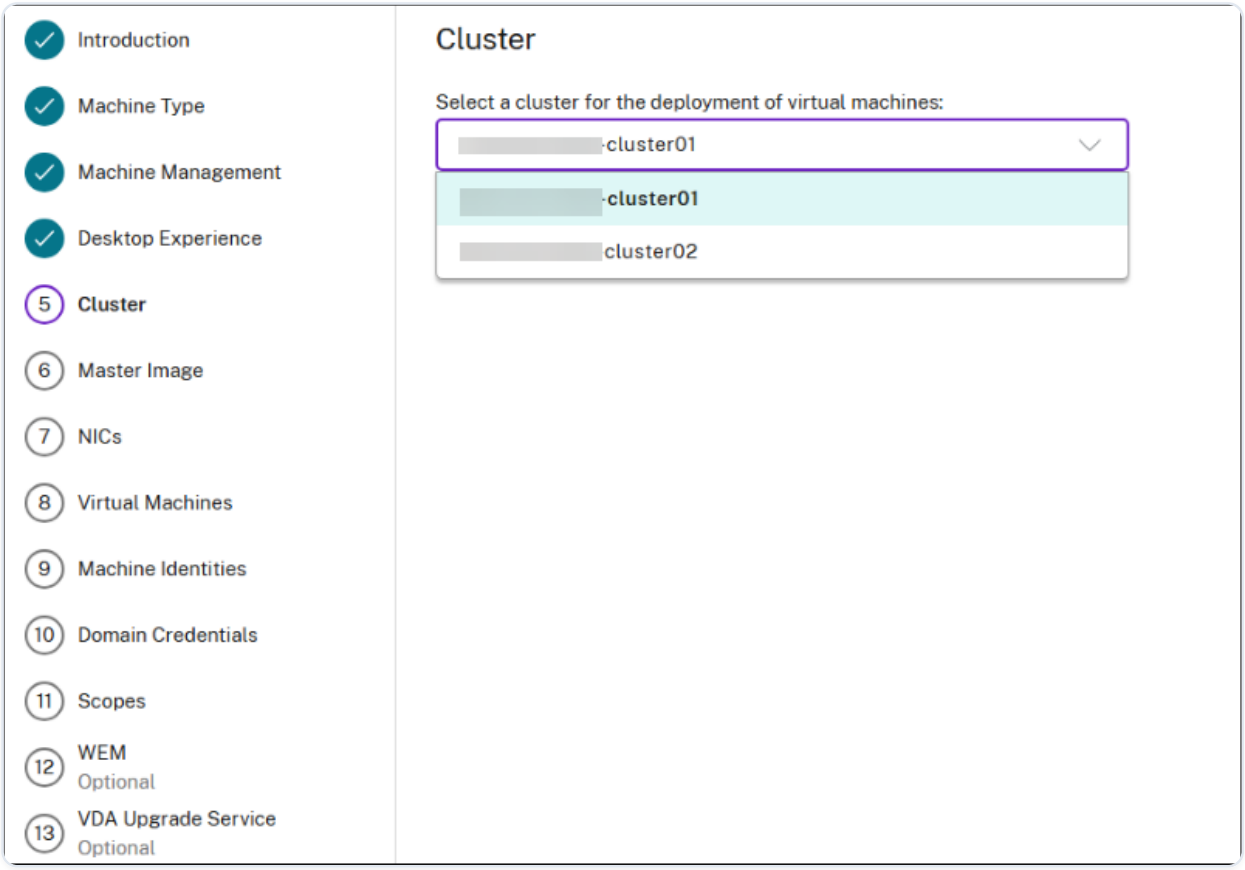
Criar um catálogo de máquinas usando o Studio

No assistente de Configuração do Catálogo de Máquinas:

1. Na página **Tipo de Máquina**, selecione **SO multissessão**, **SO de sessão única** ou **Acesso remoto a PC**.
2. Na página **Gerenciamento de Máquinas**, selecione **Máquinas com gerenciamento de energia** e **Citrix Machine Creation Services™** como método de implantação. Selecione os **Recursos**.

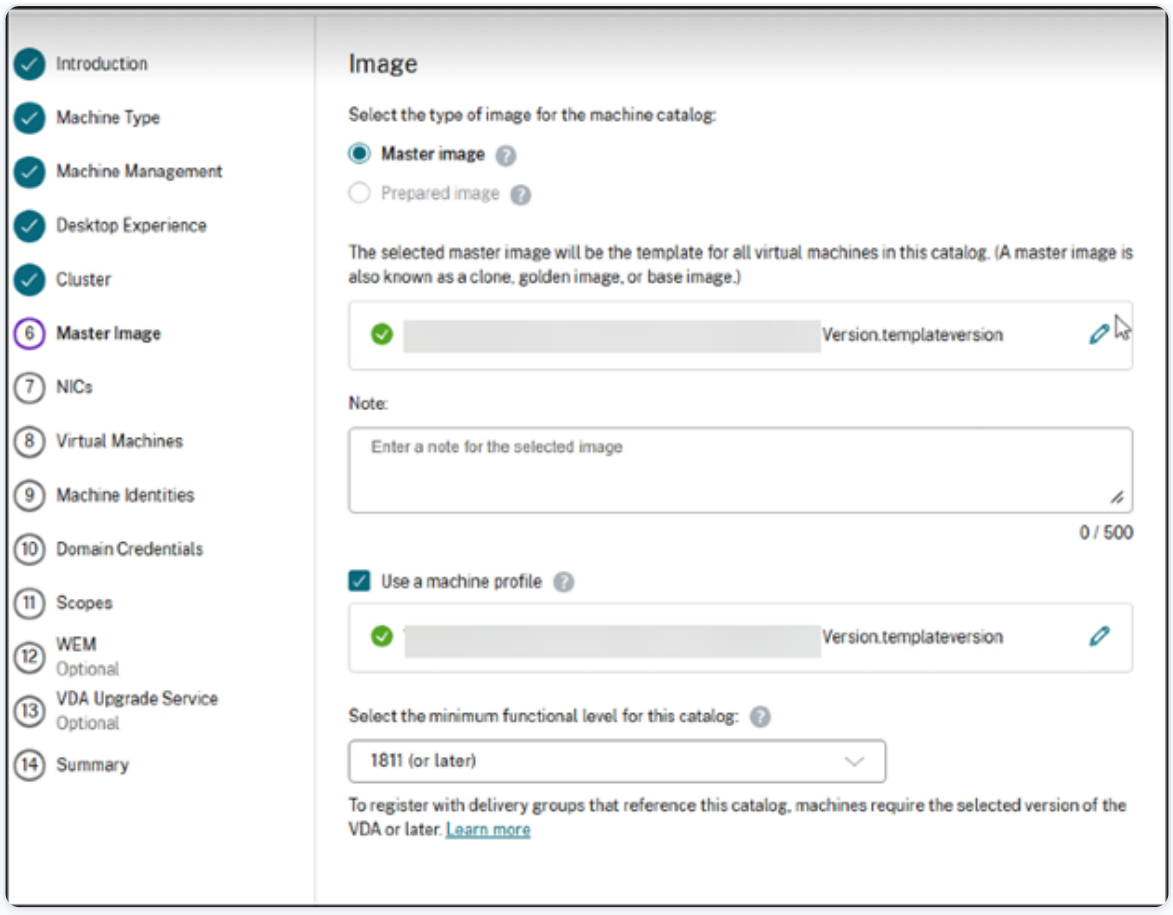


3. Na página **Experiência da Área de Trabalho**, selecione uma das duas opções.
4. Na página **Cluster**, selecione um cluster para a implantação das VMs.

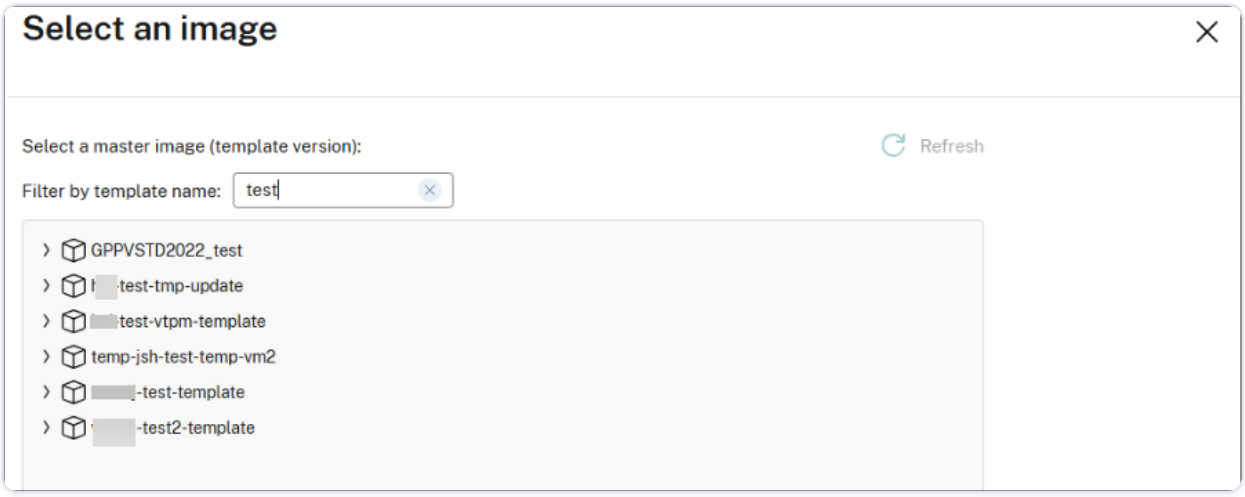


5. Na página **Imagem Mestra**, clique em **Imagem Mestra** e selecione uma imagem mestre (versão do modelo). Você pode filtrar modelos de máquina por nome. A versão do modelo da imagem mestre é definida por padrão como o perfil da máquina para novos catálogos. No entanto, você pode alterar a versão do modelo para o perfil da máquina.

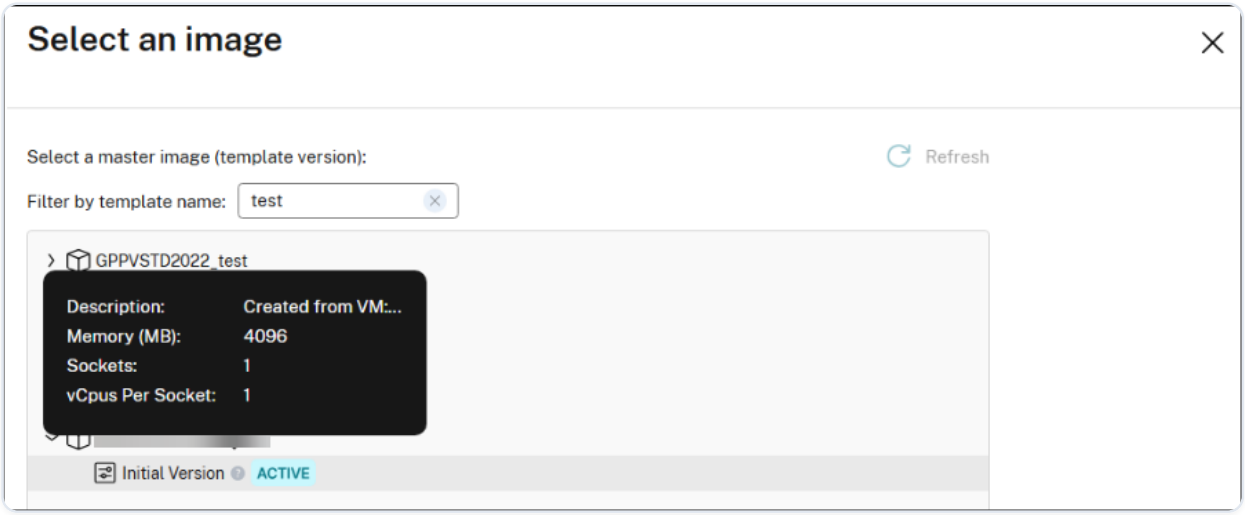
> **Nota:**
>
> Você pode usar uma única versão de modelo de VM Nutanix como VM mestre para vários catálogos de máquinas MCS, mesmo que esses catálogos estejam em clusters Nutanix diferentes.



Filtrar modelos de máquina por nome:

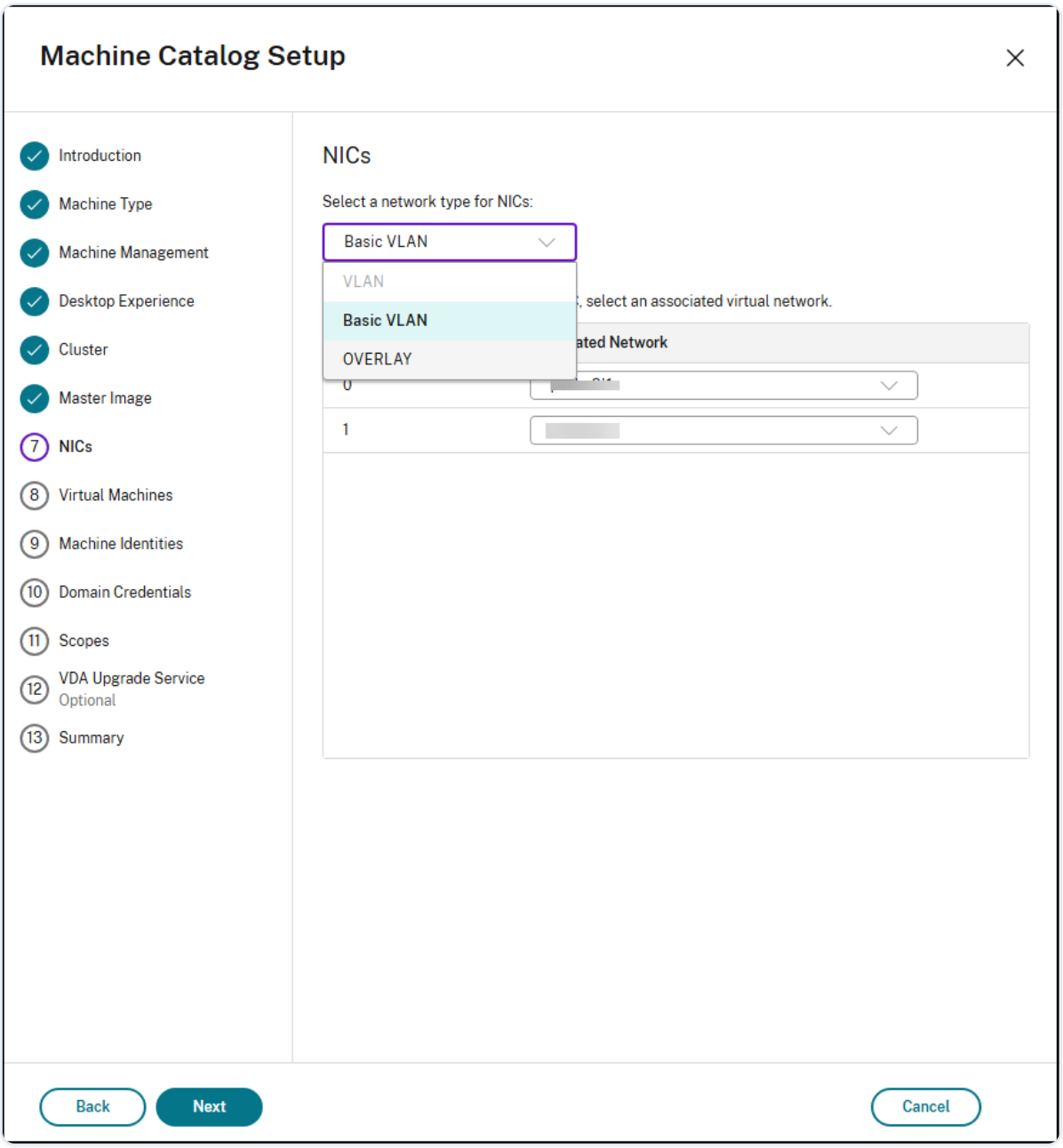


Veja a descrição de um modelo:

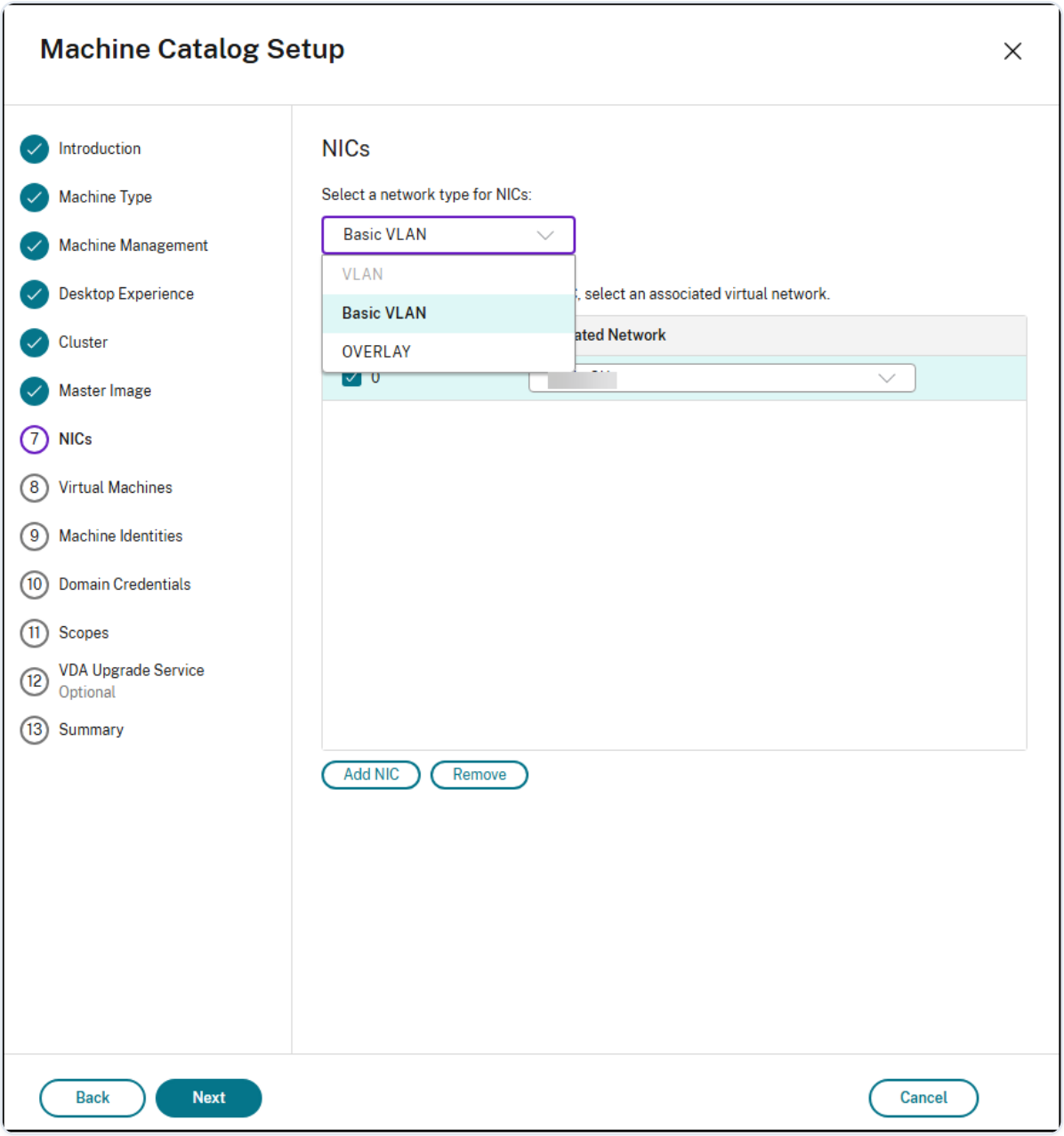


6. Na página **NICs**:

   - Selecione um tipo de NIC na lista suspensa para filtrar as redes associadas. Os tipos de rede de NICs disponíveis são: **VLAN** (VLAN Avançada), **VLAN Básica** e **OVERLAY**.
   - Se você criar um catálogo com um perfil de máquina, o número da NIC será consistente com o número da NIC do perfil de máquina e não poderá ser alterado. Selecione uma rede virtual associada para cada NIC.



- Se você criar um catálogo sem um perfil de máquina, clique em **Adicionar NIC** para aumentar a contagem de NICs ou clique em **Remover** para excluir as NICs selecionadas. Selecione uma ou mais NICs e, em seguida, selecione uma rede virtual associada para cada NIC.



7. Na página **Máquinas Virtuais**, indique o número de máquinas virtuais que você deseja criar e configure suas máquinas para Memória total (MB) em cada máquina, CPUs virtuais e Cores por CPU. Esses valores são preenchidos automaticamente a partir do perfil da máquina.
8. Na página **Resumo**, verifique os detalhes do catálogo de máquinas. Insira um nome e uma descrição para o catálogo de máquinas. Clique em **Concluir**.

EXPORTAR O PERFIL DA MÁQUINA

Você pode exportar o perfil da máquina usado pelo catálogo de máquinas para um arquivo JSON.

1. Selecione o catálogo de máquinas e navegar até a guia **Propriedades de Modelos**.
2. Em detalhes de **Perfil da Máquina**, clique em **Exportar** ao lado de **Última versão**.

Criar um catálogo de máquinas usando comandos PowerShell

1. Abra a janela do PowerShell.
2. Execute `asnp citrix*`.
3. Crie um pool de identidades se ainda não tiver sido criado. Por exemplo:

```
New-AcctIdentityPool    -Domain "<string>" -IdentityPoolName "<string>"
-IdentityType "ActiveDirectory"  -NamingScheme "DemoVM-##"
-NamingSchemeType "Numeric" -ZoneUid "GUID" -Scope @()
```

4. Crie um esquema de provisionamento.

   Por exemplo: Sem um perfil de máquina

```
New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"ClusterId`"
Value=`"00062c63-1fb0-58c9-4fc8-5c2573352378`" /><Property
xsi:type=`"StringProperty`" Name=`"CPUCores`" Value=`"1`" /></
CustomProperties>" -HostingUnitName "<Hosting unit name>"
-IdentityPoolName "<string>" -InitialBatchSizeHint 1  -MasterImageVM
"XDHyp:\HostingUnits\<Hosting Unit Name>\Templates.folder\<template
name>.template\<template version name>.templateversion" -NetworkMapping
@{"5"="XDHyp:\HostingUnits\<Hosting unit name>\Clusters.folder\<Cluster
Name>.cluster\<Network name>.network"} -ProvisioningSchemeName
"<Catalog name>" -ProvisioningSchemeType "MCS" -RunAsynchronously
-Scope @() -VMCpuCount 2 -VMMemoryMB 10240
```

   Por exemplo: Com um perfil de máquina

   Use um perfil de máquina para capturar propriedades de hardware de uma versão de modelo e aplicá-las às VMs provisionadas. Se você não especificar o perfil de máquina, as propriedades de hardware serão capturadas da versão do modelo da imagem mestre.

> **Nota:**
>
> - As propriedades de Disco do SO, vTPM e Inicialização Segura são sempre capturadas da imagem mestre, mesmo quando um perfil de máquina é usado.

- Como o Disco do SO não é lido do perfil da máquina, você pode criar uma VM sem disco e convertê-la em uma versão de modelo que pode ser usada para o perfil da máquina.
- Como a especificação JSON completa da versão do modelo de perfil de máquina é armazenada, você pode criar as VMs mesmo se excluir a versão do modelo do Prism Central.

As propriedades capturadas do perfil da máquina são:

PROPRIEDADE	NOME DA PROPRIEDADE NA API (GETTEMPLATEVERSIONBYID)	COMENTÁRIOS/ REFERÊNCIAS
CPU	**numSockets**	
RAM	**memorySizeBytes**	
Núcleo	**numCoresPerSocket**	
Categorias	**categorias**	Gerenciamento de Categorias
GPU	**GPUs**	Visualização de Resumo de GPUs
Threads por Núcleo	**numThreadsPerCore**	aCLI-VM
Nós Numa	**numNumaNodes**	
Habilitar Fixação Rígida de VCPU	**isVcpuHardPinningEnabled**	
Habilitar Passagem de CPU	**isCpuPassthroughEnabled**	
Habilitar Superalocação de Memória	**isMemoryOvercommitEnabled**	Criando uma VM através do Prism Central (AHV)

PROPRIEDADE	NOME DA PROPRIEDADE NA API (GETTEMPLATEVERSIONBYID)	COMENTÁRIOS/ REFERÊNCIAS
Habilitar Acesso ao Console da GPU	**isGpuConsoleEnabled**	
Habilitar Hot Plug de CPU	**isCpuHotplugEnabled**	
Habilitar Controlador SCSI	**isScsiControllerEnabled**	
Fuso horário	**hardwareClockTimezone**	Criando uma VM através do Prism Central (AHV)
Habilitar a marca AHV	**isBrandingEnabled**	
Habilitar Console VGA	**isVgaConsoleEnabled**	
VM	**isAgentVm**	Criando uma VM através do Prism Central (AHV)

Observação:

Usando a mesma versão do modelo de imagem mestre, você pode criar catálogos diferentes com vários perfis de máquina, cada um apresentando um conjunto distinto de propriedades mencionadas acima. Por exemplo, você pode atribuir diferentes Categorias que podem ser vinculadas a Políticas Nutanix, ajustar CPU/Memória, modificar as configurações de Memory Overcommit ou adicionar e remover várias GPUs.

Os parâmetros de linha de comando, como `VMCpuCount`, `VMMemoryMB` e `CPUCores` no `CustomProperties`, podem ser fornecidos e têm precedência sobre os valores desses parâmetros da versão do modelo de perfil da máquina. Se não forem fornecidos, eles são lidos do perfil da máquina fornecido.

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
    <StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378" />

    <StringProperty Name="CPUCores" Value="2" />

</CustomProperties>

"@



New-ProvScheme -HostingUnitName "<Hosting unit name>" `

           -IdentityPoolName "<string>" `

           -InitialBatchSizeHint 1 `

           -MasterImageVM "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<template name>.template\<template version
name>.templateversion" `

           -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<template name for machine
profile>.template\<template version name>.templateversion" `

           -NetworkMapping @{"0"="XDHyp:\HostingUnits\<Hosting unit
name>\Clusters.folder\<Cluster Name>.cluster\<Network name>.network"} `

           -ProvisioningSchemeName "<Catalog name>" `

           -ProvisioningSchemeType "MCS" `

           -CustomProperties $customProperties `

           -RunAsynchronously `

           -VMCpuCount 2 `

           -Scope @()
```

5. Registre um esquema de provisionamento como um catálogo de broker. Por exemplo:

```
New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False  -
MinimumFunctionalLevel "L7_20" -Name "<Catalog Name>"
-PersistUserChanges "Discard" -ProvisioningType "MCS"    -
SessionSupport "MultiSession" -ZoneUid "GUID"  -ProvisioningSchemeId
fe7df345-244e-4xxxx-xxxxxxxxx `  -Scope @()
```

Criar um catálogo de máquinas com máquinas existentes (gerenciadas por energia)

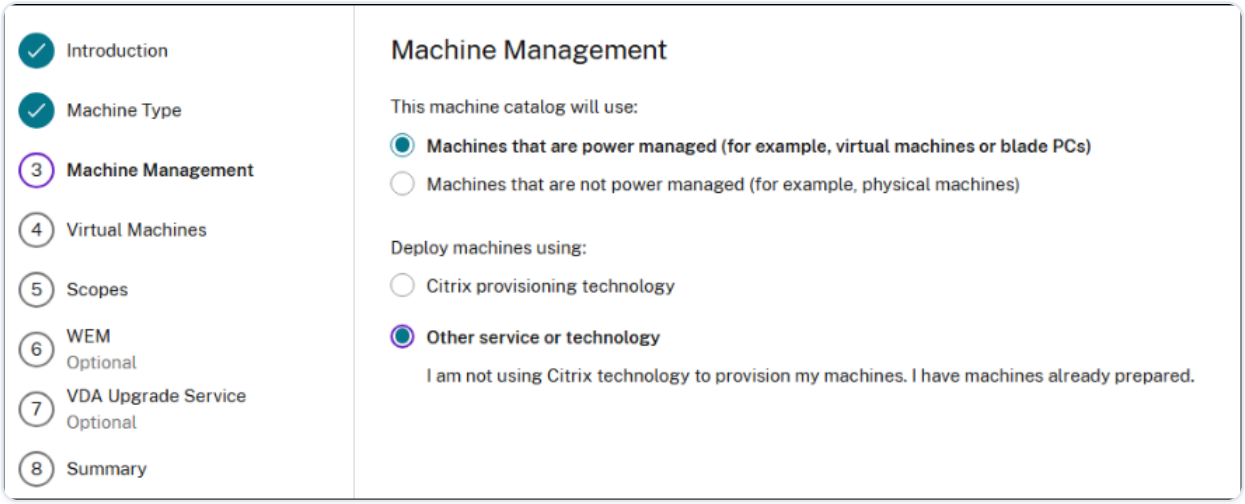
Você pode criar um catálogo de máquinas com máquinas existentes (gerenciadas por energia) usando:

- Studio
- PowerShell

Criar um catálogo de máquinas com máquinas existentes (gerenciadas por energia) usando o Studio

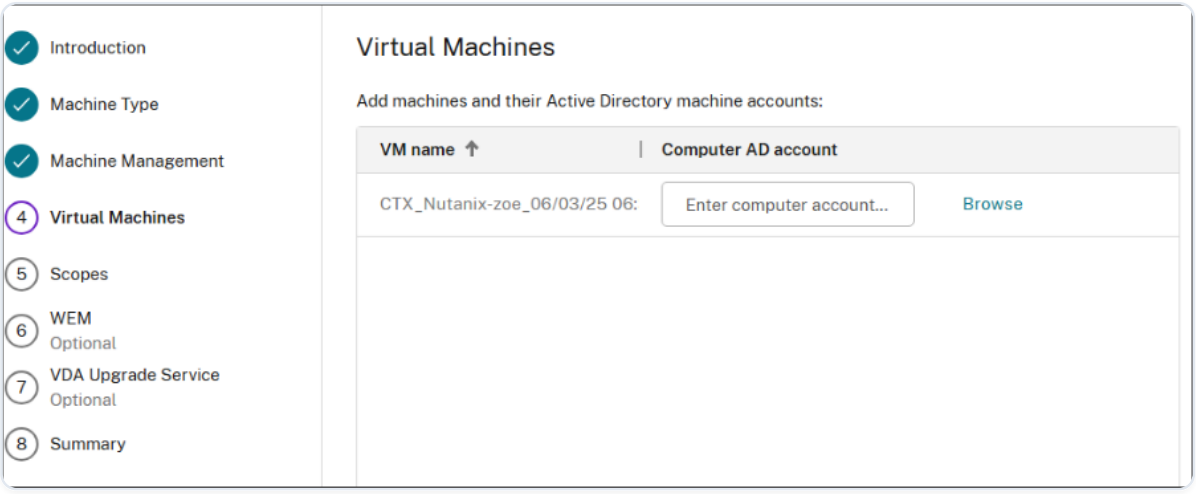
No assistente de Configuração do Catálogo de Máquinas:

1. Na página **Sistema Operacional**, selecione **SO multissessão** ou **SO de sessão única**.
2. Na página **Gerenciamento de Máquinas**, selecione **Máquinas gerenciadas por energia** e **Outro serviço ou tecnologia**.



3. Na página **Máquinas Virtuais**, adicione máquinas e suas contas de máquina do Active Directory. Você pode fazer uma das seguintes opções:
   - Clique em **Importar de arquivo CSV** para adicionar máquinas em massa. Para obter informações sobre como usar arquivos CSV para adicionar máquinas, consulte Usar arquivos CSV para adicionar máquinas em massa a um catálogo.

- Clique em **Adicionar Máquinas** para adicionar máquinas manualmente. A janela **Selecionar VMs** é exibida. Expanda a conexão do Nutanix AHV Prism Central que você criou anteriormente e selecione as VMs que deseja adicionar. Em seguida, adicione os nomes das contas de máquina associadas.



4. As páginas **Escopos** e **Resumo** não contêm informações específicas do Nutanix AHV Prism Central.

Criar um catálogo de máquinas com máquinas existentes (gerenciadas por energia) usando o PowerShell

1. Abra a janela do PowerShell.
2. Execute `asnp citrix*`.
3. Crie um catálogo para ter VMs com gerenciamento de energia atribuídas ao usuário. Por exemplo:

```
New-BrokerCatalog -AllocationType "Permanent"  -IsRemotePC $False
-MachinesArePhysical $False  -Name "<Catalog Name>" -PersistUserChanges
"OnLocal" -ProvisioningType "Manual" -Scope @() -SessionSupport
"SingleSession" -ZoneUid "fb202053-8c35-4db2-a299-a8d9538ec6be"
```

4. Adicione VMs ao catálogo. Por exemplo:

```
New-BrokerMachine  -CatalogUid 6 -HostedMachineId "d859caf3-4bf0-447b-
b012-8af0594c7d88" -HypervisorConnectionUid 1 -IsReserved $False  -
MachineName "S-1-5-21-1334627847-1250330507-3910179295-100245"
```

Criar um catálogo de máquinas usando um snapshot do Nutanix

Esta seção descreve como criar um catálogo de máquinas provisionado por MCS com conexão de host Nutanix Acropolis (Prism Element). Antes de criar o catálogo, crie imagens mestre e snapshots no Nutanix. Para obter mais informações, consulte a documentação do Nutanix.

No assistente de Configuração do Catálogo de Máquinas:

- A página **Container** ou **Cluster and Container** é exclusiva do Nutanix.
    - Se você implantar máquinas usando o Nutanix AHV XI como recursos, na página **Container**, selecione um contêiner onde os discos de identidade das VMs serão colocados.
    - Se você implantar máquinas usando o Nutanix AHV PC como recursos, verá a página **Cluster and Container**. Selecione qual cluster usar para a implantação de VMs e, em seguida, um contêiner.
- Na página **Image**, selecione o snapshot da imagem. Use o console do Acropolis para renomear seus snapshots, se necessário. Se você renomear snapshots, reinicie o assistente de criação de catálogo para ver uma lista atualizada.
- Na página **Virtual Machines**, indique o número de CPUs virtuais e o número de núcleos por vCPU.
- Na página **NICs**, selecione o tipo de NIC para filtrar as redes associadas. Esta opção está disponível apenas para conexões Nutanix AHV PC.
- As páginas **Machine Identities**, **Domain Credentials**, **Scopes** e **Summary** não contêm informações específicas do Nutanix.

Limitações

Ao criar um catálogo MCS com conexão de host Nutanix (especificamente, plug-in Nutanix AHV 2.7.1 e plug-in Nutanix AHV 2.5.1), o tamanho do disco rígido das VMs provisionadas é exibido incorretamente no Studio.

- Nutanix AHV plug-in 2.7.1: O tamanho exibido é menor (1 GB) do que o tamanho real do armazenamento.
- Nutanix AHV plug-in 2.5.1: O tamanho exibido é menor (32 GB) do que o tamanho real do armazenamento.

No entanto, isso funciona conforme o esperado se a VM da imagem mestre for um snapshot na VM.

Onde ir em seguida

- Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.
- Para revisar todo o processo de configuração, consulte Planejar e construir uma implantação.
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo Nutanix.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com Nutanix
- Conexão com a nuvem Nutanix e soluções de parceiros
- Criar catálogos de máquinas

Criar um catálogo Red Hat OpenShift

(/pt-br/citrix-daas/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização Red Hat OpenShift.

> **Nota:**

> Antes de criar um catálogo Red Hat OpenShift, conclua a criação de uma conexão e unidade de hospedagem para o Red Hat OpenShift. Consulte Conexão com Red Hat OpenShift.

Criar uma VM de imagem mestre

É necessária uma VM de imagem mestre para criar um catálogo de máquinas.

1. Acesse o Console do OpenShift usando seu ID de login.
2. navegar até **Virtualization > VirtualMachines** para ver a lista de VMs, incluindo VMs de imagem mestre.
3. Crie uma imagem mestre. Ao criar uma imagem mestre, certifique-se de que a VM da imagem mestre tenha apenas um dispositivo de armazenamento.

> **Nota:**

- Certifique-se de que um NAD roteável seja adicionado à VM da imagem mestre de acordo com os requisitos do cliente para o ambiente de cluster.
- Quando a imagem mestre é unida a um domínio, ela pode perder a confiança do domínio após ser usada para a criação do catálogo. Esse problema afeta o Citrix Virtual Apps and Desktops™ 2503 devido a uma limitação no ambiente OpenShift. A solução alternativa é não unir o domínio em imagens mestre. A Citrix está trabalhando com a Red Hat para aprimorar os recursos de isolamento de rede.
- Ao criar um catálogo de máquinas MCS em um ambiente de virtualização Red Hat OpenShift, você não pode usar uma imagem mestre e um perfil de máquina que tenham tipos de sistema operacional diferentes. Isso se deve à forma como o Red Hat OpenShift gerencia cada tipo de SO. Portanto, usar uma VM Windows como imagem mestre com uma VM não Windows (exemplo, Linux) como perfil de máquina, ou vice-versa, não é suportado.
- Atualmente, as VMs criadas usando `InstanceType` não são suportadas como uma imagem mestre.

Criar um catálogo

Você pode criar catálogos OpenShift para criar, entregar e gerenciar o consumo de energia de máquinas em seus ambientes OpenShift.

- Criar um catálogo usando o Studio
- Criar um catálogo usando comandos PowerShell

Criar um catálogo usando o Studio

Você pode criar um catálogo de máquinas MCS no ambiente Red Hat OpenShift com ou sem um perfil de máquina usando o Web Studio. Uma VM é usada como entrada de perfil de máquina.

No assistente de Configuração do Catálogo de Máquinas:

1. Na página **Sistema Operacional**, selecione **SO multissessão** ou **SO de sessão única**.
2. Na página Gerenciamento de Máquinas:
   - Selecione **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade)**.
   - Selecione para implantar máquinas usando a **tecnologia de provisionamento Citrix Machine Creation Services™ (MCS)**.

- Selecione a unidade de hospedagem Openshift em Citrix Machine Creation Services (MCS)

3. Na página **Experiência da Área de Trabalho**, selecione a opção de acordo com o tipo de máquina que você selecionou na página **Tipo de Máquina**.
4. Na página **Imagem**:

   a. Selecione uma imagem mestre. Atualmente, o Openshift não oferece suporte a imagens preparadas.

   b. Você pode adicionar uma nota para a imagem selecionada.

   c. Você pode selecionar a caixa de seleção **Usar um perfil de máquina** e selecionar um perfil de máquina.

   d. Para habilitar o uso dos recursos mais recentes do produto, certifique-se de que a imagem mestre tenha a versão mais recente do VDA instalada. Não altere a seleção mínima padrão do VDA. No entanto, se você precisar usar uma versão anterior do VDA, consulte Versões do VDA e níveis funcionais.

5. Na página **NICs**, selecione uma ou mais NICs, associe uma rede virtual a cada placa.
6. Na página **Máquinas Virtuais**:

   a. Especifique quantas máquinas virtuais criar. Digite 0 (zero) se não quiser criar nenhuma. Mais tarde, você pode criar VMs para um catálogo vazio adicionando máquinas.

   b. Escolha a quantidade de memória (em MB) que cada VM terá.

   c. Se você estiver criando um catálogo aleatório não persistente, poderá habilitar o Cache de Write-Back para máquinas para melhorar o desempenho de E/S. Consulte Configurar cache para dados temporários.

7. Siga as instruções na tela para concluir as etapas restantes, que não incluem informações específicas do OpenShift.

Você também pode usar o Studio para criar catálogos do OpenShift para entregar e gerenciar o poder das máquinas existentes em seus ambientes OpenShift. Faça o seguinte:

No assistente de Configuração do Catálogo de Máquinas:

1. Na página **Sistema Operacional**, selecione **SO multissessão** ou SO de sessão única.
2. Na página **Gerenciamento de Máquinas**, selecione **Máquinas com gerenciamento de energia e Outro serviço ou tecnologia**.

3. Na página **Máquinas Virtuais**, adicione máquinas e suas contas de máquina do Active Directory. Você pode:

   - *Adicionar máquinas manualmente*: Clique em **Adicionar Máquinas para adicionar máquinas manualmente**. A janela **Selecionar VMs** é exibida. Expanda a conexão OpenShift que você criou anteriormente e selecione os nós (VMs) que deseja adicionar. Em seguida, adicione os nomes das contas de máquina associadas.
   - *Adicionar máquinas usando um arquivo CSV*: Clique em **Adicionar Arquivo CSV para adicionar máquinas em massa**. Para obter informações sobre como usar arquivos CSV para adicionar máquinas, consulte Usar arquivos CSV para adicionar máquinas em massa a um catálogo.

4. Siga as instruções na tela para concluir as etapas restantes, que não incluem informações específicas do OpenShift.

Criar um catálogo usando comandos PowerShell

Atualmente, você pode criar um catálogo de máquinas MCS no ambiente Red Hat OpenShift usando apenas comandos PowerShell. Você pode criar o catálogo de máquinas com ou sem o uso de um perfil de máquina. Uma VM é usada como entrada de perfil de máquina.

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*`.
3. Execute comandos PowerShell para

   a. Criar um pool de identidades

   b. Criar contas AD

   c. Crie um catálogo de máquinas MCS com VMs persistentes com ou sem um perfil de máquina.

   d. Adicionar VMs ao catálogo

   e. Criar um catálogo de broker

   f. Adicionar máquinas broker às novas VMs

A seguir, um script de exemplo:

CRIAR UM POOL DE IDENTIDADES

```
New-AcctIdentityPool `

    -IdentityPoolName "IdentityPoolName" `
```

```
    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -NamingScheme "vm###" `

    -NamingSchemeType "Numeric" `

    -AllowUnicode `

    -Domain "MyDomain.local" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

CRIAR CONTAS AD

```
New-AcctADAccount `

    -IdentityPoolUid "11111111-1111-1111-1111-111111111111" `

    -ADUserName "MyDomain\MyUserName" `

    -ADPassword SecurePassword `

    -Count 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

CRIAR UM ESQUEMA DE PROVISIONAMENTO COM MÁQUINAS PERSISTENTES (SEM PERFIL DE MÁQUINA)

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `

    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`
```

```
    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `

    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

CRIAR UM ESQUEMA DE PROVISIONAMENTO COM MÁQUINAS PERSISTENTES (COM PERFIL DE MÁQUINA)

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `

    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `

    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local" `

    -MachineProfile "XDHyp:
```

```
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MachineProfileVM.v
m"
```

CRIAR NOVAS PROVVMS

```
New-ProvVM `

    ProvisioningSchemeName "ProvisioningSchemeName" `

    ADAccountName "MyDomain\vm001" `

    AdminAddress "MyDDC.MyDomain.Local"



Lock-ProvVM `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -Tag "Brokered" `

    -VMID "TargetNamespace:vm001"
```

CRIAR NOVO CATÁLOGO DE BROKER

```
New-BrokerCatalog `

    -Name "ProvisioningSchemeName" `

    -ProvisioningType "MCS" `

    -SessionSupport "MultiSession" `

    -AllocationType "Random" `

    -PersistUserChanges "OnLocal" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

DEFINIR METADADOS DO CATÁLOGO DE BROKER

```
Set-BrokerCatalogMetadata `

    -CatalogId "1" `

    -Name "Citrix_DesktopStudio_IdentityPoolUid" `

    -Value "11111111-1111-1111-1111-111111111111"



Set-BrokerCatalog `

    -Name "ProvisioningSchemeName " `

    -ProvisioningSchemeId "22222222-2222-2222-2222-222222222222"
```

CRIAR MÁQUINAS DE BROKER PARA AS NOVAS PROVVMS

```
New-BrokerMachine `

    -CatalogUid "33333333-3333-3333-3333-333333333333" `

    -AdminAddress "MyDDC.MyDomain.Local" `

    -MachineName "S-0-0-00-0000000000-0000000000-000000000-000000"
```

Próximos passos

- Se este for o primeiro catálogo criado, o Studio o guiará para Criar um grupo de entrega

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o Red Hat OpenShift
- Criar catálogos de máquinas

Criar um catálogo VMware

(/pt-br/citrix-daas/install-configure/machine-catalogs-create.html) descreve os assistentes que criam um catálogo de máquinas.

Nota:

Antes de criar um catálogo VMware, você precisa concluir a criação de uma conexão com o VMware. Consulte (/pt-br/citrix-daas/install-configure/connections/connection-vmware-virtualization-environments.html).

Criar um catálogo de máquinas usando um perfil de máquina

Você pode criar um catálogo de máquinas MCS usando um perfil de máquina. A origem da entrada do perfil de máquina é um modelo VMware. O perfil de máquina captura as propriedades de hardware de um modelo VMware e as aplica às VMs recém-provisionadas no catálogo.

Nota:

- A entrada da imagem mestre (instantâneo) e a entrada do perfil da máquina (modelo VMware) devem ter o vTPM ativado ou desativado. Esta regra se aplica a `New-ProvScheme` e `Set-ProvScheme`.
- Se a imagem mestre tiver o vTPM ativado, o modelo VMware só poderá vir da mesma origem de VM que a imagem mestre.
- A política de armazenamento criptografado suporta apenas clone completo.
- Os catálogos baseados em perfil de máquina utilizam o modelo VMware fornecido para coletar informações do controlador de armazenamento, contando com os discos virtuais anexados. O modelo deve incluir um disco virtual que é necessário para recuperar as informações do controlador de armazenamento usadas para configurar discos virtuais para as máquinas virtuais.

O modelo VMware no perfil da máquina deve existir durante o ciclo de vida do catálogo para permitir o provisionamento de VMs para o catálogo. Sem um modelo VMware, você não pode provisionar novas VMs. Quando um modelo VMware é excluído, você deve fornecer um novo modelo usando o comando `Set-ProvScheme`.

- O MCS captura as propriedades de um modelo VMware. Você pode criar um novo modelo VMware referenciando as propriedades armazenadas do modelo VMware usando o comando `Get-Provscheme`.

- Alternativamente, se o catálogo de máquinas e as VMs provisionadas existirem, uma máquina provisionada pelo MCS também poderá ser usada para criar um novo modelo VMware.
- Quando o MCSIO está ativado, você pode atualizar os tamanhos da memória e do cache de disco após criar os catálogos MCS.

Com base em diferentes sistemas operacionais, você pode criar um catálogo de máquinas com diferentes configurações:

- Se o Windows 11 estiver instalado na imagem mestre, é um requisito ter o vTPM habilitado para a imagem mestre. Portanto, o modelo VMware, que é uma fonte de perfil de máquina, deve ter o vTPM anexado a ele.
- Se o Windows 10 estiver instalado na imagem mestre sem vTPM anexado, você pode criar um catálogo de máquinas com um modelo VMware sem vTPM como fonte para o perfil da máquina.

Existe outra configuração onde você pode criar um catálogo de máquinas usando o modo de disco de cópia completa com um modelo de perfil de máquina aplicado com política de armazenamento criptografado.

Para criar um catálogo de máquinas usando comandos PowerShell com perfil de máquina como entrada:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute os seguintes comandos:
    - Para criar um catálogo de máquinas com um modelo VMware com vTPM anexado como fonte para entrada de perfil de máquina e imagem mestre com Windows 11 instalado:

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name"
```

```
-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "vSanRg"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4  -VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<catalog name>"
-ProvisioningType 'MCS'

-Scope @()  -SessionSupport "SingleSession"
```

```
-ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- Para criar um catálogo de máquinas com um modelo VMware sem vTPM como fonte para perfil de máquina e imagem mestre com Windows 10 instalado:

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"
```

```
-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"  -Description "<string>"  -IsRemotePC
$False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()  -SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- Para criar um catálogo de máquinas usando o modo de disco de cópia completa com um modelo de perfil de máquina aplicado com política de armazenamento criptografado:

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"
```

```
-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"

-UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- Para atualizar um perfil de máquina, use o comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName
'name' -MachineProfile 'XDHyp:\HostingUnits\<hosting unit
name>\<template name>.template
```

Verificar várias NICs

Você recebe várias mensagens de erro durante as verificações pré-voo para várias NICs ao usar um perfil de máquina e o parâmetro `NetworkMapping` nos comandos `New-ProvScheme` e `Set-ProvScheme`.

A lista de verificação pré-voo para várias NICs é a seguinte:

- Apenas a contagem de NICs do modelo de perfil da máquina é usada e validada. A rede para a qual essas NICs apontam não é usada nem validada em relação às redes da unidade de hospedagem.
- Se a contagem de NICs no modelo de perfil da máquina for maior que o número de redes na unidade de hospedagem, você receberá uma mensagem de erro.
- Se a contagem de NICs no modelo de perfil da máquina for zero, você receberá uma mensagem de erro. Quando a contagem de NICs no modelo de perfil da máquina for um, então:
  - Se nenhum mapeamento de rede for especificado no comando `New-ProvScheme` ou `Set-ProvScheme`, e a rede da unidade de hospedagem for uma, então a rede da unidade de hospedagem será usada.
  - Se um mapeamento de rede for especificado, então o mapeamento de rede especificado será usado, se for válido.
- Quando a contagem de NICs no modelo de perfil da máquina for maior que 1, ou a contagem de redes da unidade de hospedagem for maior que 1, então:
  - É necessário um mapeamento de rede válido no comando, e ele deve fornecer mapeamento para cada NIC (ou seja, a contagem de NetworkMapping deve ser a mesma que a contagem de NICs do perfil da máquina).
  - Várias NICs não podem ser mapeadas para a mesma rede na unidade de hospedagem.
  - A contagem de `NetworkMapping` e a contagem de NICs do perfil da máquina devem ser menores ou iguais à contagem de redes da unidade de hospedagem.
  - `NetworkMapping` deve ser fornecido para cada ID de 0 a n-1, onde n é o número de adaptadores de rede no modelo de perfil da máquina.

Provisionar um disco de dados em VM criada por MCS

Um disco de dados permite o armazenamento de dados persistentes como logs de eventos, rastreamentos de segurança e dados de aplicativos. Você pode criar e atribuir um disco de dados

persistente ou não persistente a uma VM persistente ou não persistente criada por MCS de um catálogo de máquinas MCS no VMware.

Provisione o disco de dados a partir da imagem mestre. O disco de dados da imagem mestre preparada é armazenado na pasta `<Prov Scheme Name>-dataDisk-<datastoreId>`.

Você pode criar um catálogo MCS baseado em perfil de máquina e não baseado em perfil de máquina. Para o catálogo MCS baseado em perfil de máquina, você pode usar a mesma VM de imagem mestre como fonte do disco de dados para o perfil da máquina.

O disco de dados da VM provisionada deriva propriedades como política de armazenamento e tamanho da imagem mestre. Para o catálogo baseado em perfil de máquina, ele pode opcionalmente usar o disco de dados do modelo de VM para derivar as propriedades. Se o modelo de VM não tiver um disco de dados, a política padrão do armazenamento será usada.

O disco de dados da VM provisionada é criado no mesmo diretório que o disco do SO e de Identidade.

Cenários de disco de dados suportados

A seguir estão os cenários de disco do SO e de disco de dados suportados:

- Disco do SO persistente com disco de dados persistente
- Disco do SO não persistente com disco de dados persistente
- Disco do SO não persistente com disco de dados não persistente

> **Nota:**
>
> Um catálogo de máquinas persistente não pode ter um disco de dados não persistente.

Limitações

As seguintes operações não são atualmente suportadas:

- Provisionamento de mais de um disco de dados.
- Redefinir o disco de dados.
- Atualizar um catálogo MCS com um disco de dados para um catálogo MCS sem disco de dados. Da mesma forma, atualizar um catálogo MCS sem um disco de dados para um catálogo MCS com disco de dados.

Etapas principais

1. Crie uma VM de imagem mestre com um disco de dados no VMware. Para um catálogo MCS baseado em perfil de máquina, você pode usar a mesma VM de imagem mestre como a origem do disco de dados para o perfil de máquina.
2. Crie um catálogo de máquinas MCS com VMs provisionadas com disco de dados usando o comando PowerShell `New-ProvScheme`. Consulte Criar um catálogo com VMs provisionadas com disco de dados.
3. Adicione VMs ao catálogo usando o comando PowerShell `New-ProvVM`.
4. Faça login na VM para verificar se o disco de dados está formatado corretamente. Se houver conteúdo no disco de dados referenciado na VM da imagem mestre, esse conteúdo também estará no disco de dados.

Crie uma VM de imagem mestre com disco de dados no VMware

1. Crie uma VM com dois discos rígidos. Um é o disco do SO e o segundo é o disco de dados. Siga este guia para adicionar um Novo Disco Rígido (disco de dados) a uma VM existente.
2. Faça login na VM para inicializar o disco, definir a letra da unidade desejada e adicionar o conteúdo.

Crie um catálogo com VMs provisionadas com disco de dados

Inclua os seguintes parâmetros no comando PowerShell `New-ProvScheme` para provisionar um catálogo de máquinas MCS com disco de dados.

- `DataDisk`: Para especificar o caminho do disco de dados especificado.
- `DataDiskPersistence`: Para indicar se o DataDisk é persistente ou não persistente.

  O disco de dados não pode ser não persistente se `CleanOnBoot` for falso. Você não pode alterar o valor de `DataDiskPersistence` para um catálogo de máquinas depois de configurado.

Depois de criar o catálogo, adicione VMs usando o comando `New-ProvVM`.

Atualização de imagem

Execute o comando `Publish-ProvMasterVMImage` para atualizar a origem do SO e do disco de dados. Após executar o comando `Publish-ProvMasterVMImage`:

- As novas VMs são criadas com o SO e os discos de dados atualizados.
- Os discos não persistentes das VMs existentes são atualizados no próximo ciclo de energia.

- Os discos persistentes das VMs existentes não são atualizados no próximo ciclo de energia.

Excluir o disco de dados

Se você excluir o catálogo, o disco de dados será excluído, a menos que você use a opção `forgetVM` ou `purgeDBOnly`. Se você excluir a VM, o disco de dados será excluído, a menos que você use a opção `forgetVM` ou `purgeDBOnly`. Essas condições são aplicáveis apenas a catálogos de máquinas MCS persistentes.

Solução de problemas

Se o catálogo não for criado, consulte CTX294978.

Próximos passos

- Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.
- Para revisar todo o processo de configuração, consulte Planejar e criar uma implantação.
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo VMware.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com VMware
- Conexão com soluções de nuvem e parceiros VMware
- Criar catálogos de máquinas

Criar um catálogo XenServer®

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização XenServer (anteriormente Citrix Hypervisor).

> **Nota:**
>
> Antes de criar um catálogo XenServer, você precisa concluir a criação de uma conexão com o XenServer. Consulte Conexão com o XenServer.

Criar um catálogo de máquinas usando um XenServer com capacidade de GPU

Máquinas com capacidade de GPU exigem uma imagem mestre dedicada. Essas VMs exigem drivers de placa de vídeo que suportem GPUs. Configure máquinas com capacidade de GPU para permitir que a VM opere com software que usa a GPU para operações.

1. No XenCenter®, crie uma VM com VGA padrão, redes e vCPU.
2. Atualize a configuração da VM para habilitar o uso de GPU (seja Passthrough ou vGPU).
3. Instale um sistema operacional compatível e habilite o RDP.
4. Instale o Citrix VM Tools e os drivers NVIDIA.
5. Desative o Console de Administração do Virtual Network Computing (VNC) para otimizar o desempenho e, em seguida, reinicie a VM.
6. Você será solicitado a usar o RDP. Usando o RDP, instale o VDA e, em seguida, reinicie a VM.
7. Opcionalmente, crie um snapshot para a VM como um modelo de linha de base para outras imagens mestre de GPU.
8. Usando o RDP, instale aplicativos específicos do cliente que são configurados no XenCenter e usam recursos de GPU.

Criar um catálogo de máquinas baseado em perfil de máquina usando PowerShell

Quando você cria um catálogo para provisionar máquinas usando MCS, você pode usar um perfil de máquina para capturar as propriedades de hardware de uma máquina virtual e aplicá-las a VMs recém-provisionadas no catálogo. Se o parâmetro `MachineProfile` não for usado, as propriedades de hardware são capturadas da VM da imagem mestre ou do snapshot.

Você também pode criar um catálogo de máquinas MCS usando um perfil de máquina que está habilitado com vTPM. Isso ajuda a criar catálogos de máquinas de VMs do Windows 11 com vTPM habilitado.

> **Nota:**
>
> - Atualmente, você pode usar apenas um snapshot como entrada de perfil de máquina.
> - Se a entrada da imagem mestre estiver com vTPM habilitado, a entrada do perfil da máquina também deve estar com vTPM habilitado. Esta regra se aplica a `New-ProvScheme` e `Set-ProvScheme`.

- Se a imagem mestre estiver com vTPM habilitado, o perfil da máquina só poderá vir da mesma fonte de VM que a imagem mestre.
- Na criação do catálogo, o vTPM da VM deve ser o mesmo vTPM que está em uso para o snapshot da imagem mestre.

Você pode atualizar os tamanhos da memória e do cache de disco após criar os catálogos MCS quando o MCSIO estiver habilitado. Você pode configurar explicitamente os seguintes parâmetros para sobrescrever os valores dos parâmetros na entrada do perfil da máquina:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

Criar um catálogo com um perfil de máquina

1. Abra a janela do PowerShell.
2. Execute `asnp citrix*`.
3. Crie um pool de identidades. O pool de identidades é um contêiner para as contas do Active Directory (AD) das VMs a serem criadas. Por exemplo:

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
"ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
"Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. Crie as contas de computador AD necessárias no Active Directory.

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -Force

New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count 10
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. Execute o comando `New-ProvScheme` para criar um catálogo. Por exemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm\ExampleSnapsh
ot.snapshot"
```

6. Registre o esquema de provisionamento como um catálogo de broker. Por exemplo:

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. Adicione VMs ao catálogo.

Atualizar um catálogo com um novo perfil de máquina

Nota:

- O comando `Set-ProvScheme`, neste caso, não altera o perfil de máquina das VMs existentes no catálogo. Somente as VMs recém-criadas adicionadas ao catálogo terão o novo perfil de máquina.

- Não é possível converter um catálogo de máquinas baseado em perfil de máquina para um catálogo de máquinas não baseado em perfil de máquina.

Para atualizar um catálogo com um novo perfil de máquina:

1. Execute o comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

   Para obter mais informações sobre o comando Set-ProvScheme, consulte Set-ProvScheme.

Onde ir em seguida

- Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.
- Para revisar todo o processo de configuração, consulte Planejar e criar uma implantação.
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo XenServer.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com XenServer
- Criar catálogos de máquinas

Pools de identidade de diferentes tipos de junção de identidade de máquina

Usando o MCS, você pode provisionar máquinas como não unidas ao domínio, unidas ao AD local, unidas ao Microsoft Entra ou unidas ao Microsoft Entra híbrido.

Para obter informações sobre como configurar identidades de máquina no Studio, consulte Criar catálogos de máquinas.

Para obter informações específicas sobre como criar pools de identidade de diferentes tipos de junção de identidade de máquina, consulte o seguinte:

- Pool de identidade de máquina unida ao Active Directory local
- Pool de identidade de máquina unida ao Microsoft Entra
- Pool de identidade de máquina unida ao Microsoft Entra híbrido
- Pool de identidade de máquina habilitada para Microsoft Intune
- Pool de identidade de máquina não unida ao domínio

Pool de identidades de máquinas unidas ao Active Directory local

Este artigo descreve como criar um pool de identidades de máquinas unidas ao Active Directory local usando o Citrix DaaS.

Usar o Studio

As informações a seguir são um suplemento às orientações em Criar catálogos de máquinas.

No assistente de criação de catálogo:

1. Na página **Identidades da Máquina**:
    a. Selecione o tipo de identidade como **Active Directory local**.
    b. Selecione uma opção de conta do Active Directory:
        - **Criar novas contas do Active Directory**:
            - Se você selecionar **Criar novas contas do Active Directory** e usar um pool de identidades existente para criar novas contas, selecione um domínio para essas contas e especifique um esquema de nomenclatura de conta.

              Para encontrar um domínio específico rapidamente, digite o nome do domínio na caixa de pesquisa na parte superior do menu suspenso **Local (domínio)** e clique em **Enter**. O **Web Studio** mostra um indicador de progresso enquanto recupera o domínio correspondente.
            - Se você selecionar **Criar novas contas do Active Directory** e usar um pool de identidades existente para criar novas contas, selecione um pool de identidades na lista.
        - **Usar contas existentes do Active Directory**: Você pode navegar ou importar de um arquivo CSV e redefinir a senha ou especificar a mesma senha para todas as contas.
    c. Clique em **Avançar**.

2. Na página **Credenciais de domínio**, selecione uma conta de serviço ou insira as credenciais manualmente. Para obter informações sobre contas de serviço, consulte Contas de serviço do Active Directory local.

Modificar a associação da conta de serviço

Para alterar a conta de serviço associada ou adicionar uma associação a um catálogo de máquinas MCS existente, use a página **Editar Catálogo de Máquinas**.

- Para adicionar uma conta de serviço, clique em **Selecionar conta de serviço** na página **Conta de Serviço**.
- Para alterar a associação da conta de serviço, clique no ícone de edição na página **Conta de Serviço**.

Usar PowerShell

Você pode associar uma conta de serviço local a um catálogo de máquinas criado pelo MCS associando uma conta de serviço local ao pool de identidades. Você pode criar um pool de identidades ou atualizar um pool de identidades existente para associá-lo a uma conta de serviço.

Por exemplo: Para criar um novo pool de identidades e associá-lo a uma conta de serviço, execute o seguinte:

```
New-AcctIdentityPool -IdentityType ActiveDirectory -IdentityPoolName
MyPool -NamingScheme Acc#### -Domain MyDomain.com -NamingSchemeType
Numeric -OU "CN=MyOU,DC=MyDomain,DC=com" -ServiceAccountUid
$serviceAccountUid
```

Por exemplo: Para atualizar um pool de identidades existente para associá-lo a uma conta de serviço, execute o seguinte:

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid

Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid -ServiceAccountUid
$serviceAccountUid
```

Nota:

> O `$serviceAccountUid` deve ser um UID válido de uma conta de serviço do Active Directory local.

Mais informações

- Contas de serviço para gerenciamento de identidade de máquina
- Contas de serviço do Active Directory local

Pool de identidades de máquinas com identidade associada ao Microsoft Entra

Este artigo descreve como criar um pool de identidades de máquinas com identidade associada ao Microsoft Entra usando o Citrix DaaS.

Para obter informações sobre requisitos, limitações e considerações, consulte Associado ao Microsoft Entra.

Antes de criar o catálogo de máquinas, você precisa do seguinte:

1. Novo local de recurso
    - navegar para a UI de administração do Citrix Cloud™ > menu hambúrguer superior esquerdo > **Locais de Recursos**.
    - Clique em **+ Local de Recurso**.
    - Insira um nome para o novo local de recurso e clique em **Salvar**.
2. Crie uma conexão de hospedagem. Consulte a seção Criar e gerenciar conexões para obter detalhes. Ao implantar máquinas no Azure, consulte Conexão com o Azure Resource Manager.

Você pode criar catálogos associados ao Microsoft Entra usando o Studio ou o PowerShell.

Usar o Studio

As informações a seguir são um suplemento às orientações em Criar catálogos de máquinas. Para criar catálogos associados ao Microsoft Entra, siga as orientações gerais desse artigo, observando os detalhes específicos dos catálogos associados ao Microsoft Entra.

No assistente de criação de catálogo:

1. Na página **Imagem**:
    - Selecione 2106 ou posterior como o nível funcional.

- Selecione **Usar um perfil de máquina** e selecione a máquina apropriada da lista.

2. Na página **Identidades da Máquina**:

   a. Selecione **Ingressado no Microsoft Entra**. As máquinas criadas são de propriedade de uma organização e são acessadas com uma conta do Microsoft Entra que pertence a essa organização. Elas existem apenas na nuvem.

   > **Nota:**
   >
   > - O tipo de identidade **Ingressado no Microsoft Entra** requer a versão 2106 ou posterior como nível funcional mínimo para o catálogo.
   > - As máquinas são ingressadas no domínio Microsoft Entra associado ao locatário ao qual a conexão de hospedagem está vinculada.

   b. Clique em **Selecionar conta de serviço** e selecione uma conta de serviço disponível na lista. Se uma conta de serviço adequada não estiver disponível para o locatário do Microsoft Entra ao qual as identidades da máquina serão ingressadas, você poderá criar uma conta de serviço. Para obter informações sobre a conta de serviço, consulte Contas de serviço do Microsoft Entra.

   > **Nota:**
   >
   > A conta de serviço que você selecionou pode estar em um status não íntegro devido a vários motivos. Você pode ir para **Administradores > Contas de Serviço** para visualizar detalhes e corrigir os problemas de acordo com as recomendações. Alternativamente, você pode prosseguir com a operação do catálogo de máquinas e corrigir os problemas mais tarde. Se você não corrigir o problema, dispositivos ingressados no Microsoft Entra ou registrados no Microsoft Intune obsoletos serão gerados, o que pode bloquear o ingresso das máquinas no Microsoft Entra.

   c. Clique em **Adicionar Atributos de Extensão** para armazenar dados exclusivos e personalizados diretamente em seus objetos de dispositivo do Entra ID. Na página **Adicionar Atributos de Extensão**, adicione **Atributos de extensão** e **Valor**.

> **Nota:**
>
> - Você pode adicionar um máximo de 15 atributos de extensão.
> - O nome deve ser exclusivo e o valor não pode estar vazio.

d. Selecione uma opção de conta do Active Directory:

- **Criar novas contas do Active Directory**:
  - Se você selecionar **Criar novas contas do Active Directory** e usar um pool de identidades existente para criar novas contas, selecione um domínio para essas contas e especifique um esquema de nomenclatura de conta.
  - Se você selecionar **Criar novas contas do Active Directory** e usar um pool de identidades existente para criar novas contas, selecione um pool de identidades na lista.
- **Usar contas existentes do Active Directory**: Você pode procurar ou importar de um arquivo CSV e redefinir a senha ou especificar a mesma senha para todas as contas.

- Especifique um esquema de nomenclatura de conta.

Os usuários devem ter acesso explícito concedido no Azure para fazer login nas máquinas usando suas credenciais do Microsoft Entra. Consulte a seção Microsoft Entra joined para obter mais detalhes.

Adicionar ou modificar atributos de extensão

Para alterar ou adicionar atributos de extensão adicionais a um catálogo de máquinas MCS existente, ou adicionar atributos de extensão a um catálogo MCS sem uma conta de serviço, use o assistente **Editar Catálogo de Máquinas**.

- Para alterar ou adicionar atributos de extensão adicionais, navegar até a página **Atributos de Extensão de Dispositivo do Microsoft Entra**. Clique no ícone de lápis e adicione ou atualize os atributos de extensão.
- Para adicionar atributos de extensão a um catálogo MCS sem uma conta de serviço do Microsoft Entra:

a. navegar até a página **Conta de Serviço**. Selecione uma conta de serviço do Microsoft Entra para o Microsoft Intra ID.

b. Vá para a página Atributos de Extensão de Dispositivo do Microsoft Entra, clique em **Adicionar Atributos de Extensão**.

Modificar a associação da conta de serviço

Para alterar a conta de serviço associada ou adicionar uma associação a um catálogo de máquinas MCS existente, use a página **Editar Catálogo de Máquinas**.

- Para adicionar uma conta de serviço, clique em **Selecionar conta de serviço** na página **Conta de Serviço**.
- Para alterar a associação da conta de serviço, clique no ícone de edição na página **Conta de Serviço**.

Usar PowerShell

A seguir estão as etapas do **PowerShell** equivalentes às operações no Studio.

A diferença entre catálogos unidos ao AD local e catálogos unidos ao Microsoft Entra reside na criação do pool de identidades e no esquema de provisionamento.

Você deve associar uma conta de serviço do Microsoft Entra ao pool de identidades e, em seguida, criar o catálogo de máquinas. Você pode criar um novo pool de identidades ou atualizar um pool de identidades existente para associá-lo a uma conta de serviço.

Criar novo pool de identidades

Por exemplo: Para criar um novo pool de identidades e associá-lo a uma conta de serviço, execute o seguinte:

```
New-AcctIdentityPool -IdentityType AzureAD -IdentityPoolName MyPool
-NamingScheme Acc#### -NamingSchemeType Numeric -ServiceAccountUid
$serviceAccountUid
```

Por exemplo: Para criar um novo pool de identidades com atributos de extensão especificados e associá-lo a uma conta de serviço, execute o seguinte:

```
New-AcctIdentityPool -IdentityPoolName MyPool -NamingScheme ACC####
-NamingSchemeType Numeric -Domain "abc.local" -IdentityType AzureAD
-ServiceAccountUid $serviceAccountUid -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

Quando uma VM é ligada pela primeira vez, após ingressar no Microsoft Entra ID, a VM reporta seu deviceId do Entra ID ao MCS.

Por exemplo: Para verificar o `EntraIDDeviceID`, execute `Get-AcctADAccount` ou `Get-AcctIdentity`.

```
Get-AcctADAccount -IdentityPoolName MyPool
```

Após a reinicialização, para VMs persistentes, o `EntraIDDeviceID` permanece o mesmo. Para VMs não persistentes, há um novo `EntraIDDeviceID` após cada reinicialização.

Nota:

O MCS remove automaticamente os atributos de extensão associados quando você exclui uma VM do catálogo, mas não a exclui do Azure.

Atualizar pool de identidades existente

Por exemplo: Para atualizar um pool de identidades existente para associá-lo a uma conta de serviço, execute o seguinte:

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid

Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid -ServiceAccountUid
$serviceAccountUid
```

Nota:

O `$serviceAccountUid` deve ser um UID válido de uma conta de serviço do Microsoft Entra.

Por exemplo: Para editar atributos de extensão para o catálogo existente, execute o seguinte:

Nota:

- Após atualizar as VMs do catálogo existente para a versão VDA 2511 ou posterior, é necessário reiniciar. Essa reinicialização permite que a VM relate seu deviceId do Entra ID ao MCS, permitindo que o MCS configure os atributos de extensão da VM.
- O catálogo existente deve ter um tipo de conta de serviço AzureAD com permissão "Device.ReadWrite.All".

Para adicionar novos atributos:

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

Para remover alguns atributos existentes

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{}
```

OU

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{extensionAttribute1 = ""; extensionAttribute2 = ""}
```

`Set-AcctIdentityPool` também atualiza os atributos de extensão do dispositivo Entra ID para VMs que já estão unidas ao Entra ID e possuem um valor `EntraIDDeviceID` em suas identidades.

Criar catálogos unidos ao Microsoft Entra

Para criar um esquema de provisionamento para catálogos unidos ao Microsoft Entra, o parâmetro **MachineProfile** é necessário em `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`"
Name=`"UseManagedDisks`" Value=`"true`" /><Property
xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"StandardSSD_LRS`" /><Property xsi:type=`"StringProperty`"
Name=`"LicenseType`" Value=`"Windows_Server`" /></CustomProperties>"
```

```
-HostingUnitName "AzureResource" -IdentityPoolName "AzureADJoinedCatalog"
-InitialBatchSizeHint 1 -MachineProfile "XDHyp:
\HostingUnits\AzureResource\image.folder\azuread-
rg.resourcegroup\MasterVDA.vm" -MasterImageVM "XDHyp:
\HostingUnits\AzureResource\image.folder\azuread-rg.resourcegroup\azuread-
small_OsDisk_1_5fb42fadf7ff460bb301ee0d56ea30da.manageddisk"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\AzureResource\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\azuread-rg.resourcegroup\azuread-
vnet.virtualprivatecloud\Test_VNET.network"} -ProvisioningSchemeName
"AzureADJoinedCatalog" -RunAsynchronously -Scope @() -SecurityGroup @()
-ServiceOffering "XDHyp:
\HostingUnits\AzureResource\serviceoffering.folder\Standard_DS1_v2.service
offering"
```

Para criar um catálogo Microsoft Entra usando uma imagem preparada. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
<preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid> -IdentityPoolUid
<IdentityPoolUid> [-CleanOnBoot] -NetworkMapping @{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.folder
\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<sunNetN
ame>.network"} -ServiceOffering <serviceofferingPath> [-MachineProfile
<machineProfilePath>] [-CustomProperties <>]
```

Visualizar o status do processo de união ao Microsoft Entra

No Studio, o status do processo de união ao Microsoft Entra é visível quando as máquinas unidas ao Microsoft Entra em um grupo de entrega estão em estado ligado. Para visualizar o status, use Pesquisar para identificar essas máquinas e, em seguida, para cada uma, verifique **Identidade da Máquina** na guia **Detalhes** no painel inferior. As seguintes informações podem aparecer em **Identidade da Máquina**:

- Unido ao Microsoft Entra
- Ainda não ingressado no Microsoft Entra ID

> **Nota:**

> Se as máquinas não conseguirem entrar no estado de ingresso no Microsoft Entra, elas não se registrarão no Delivery Controller. O status de registro delas aparecerá como **Inicialização.**

> Além disso, usando o Studio, você pode descobrir por que as máquinas estão indisponíveis. Para fazer isso, clique em uma máquina no nó **Pesquisar**, verifique **Registro** na guia **Detalhes** no painel inferior e, em seguida, leia a dica de ferramenta para obter informações adicionais.

Grupo de Entrega

Consulte a seção Criar grupos de entrega para obter detalhes.

Habilitar Rendezvous

Depois que o grupo de entrega for criado, você poderá habilitar o Rendezvous. Consulte Rendezvous V2 para obter detalhes.

Solução de problemas

Se as máquinas não conseguirem ingressar no Microsoft Entra, faça o seguinte:

- Verifique se a identidade gerenciada atribuída ao sistema está habilitada para as máquinas. As máquinas provisionadas por MCS devem ter isso habilitado automaticamente. O processo de ingresso no Microsoft Entra falha sem uma identidade gerenciada atribuída ao sistema. Se a identidade gerenciada atribuída ao sistema não estiver habilitada para máquinas provisionadas por MCS, a possível razão é:
  - `IdentityType` do pool de identidades associado ao esquema de provisionamento não está definido como `AzureAD`. Você pode verificar isso executando `Get-AcctIdentityPool`.
- Para catálogos que usam imagens mestre com VDA versão 2206 ou anterior, verifique o status de provisionamento da extensão **AADLoginForWindows** para as máquinas. Se a extensão **AADLoginForWindows** não existir, as possíveis razões são:
  - `IdentityType` do pool de identidades associado ao esquema de provisionamento não está definido como `AzureAD`. Você pode verificar isso executando `Get-AcctIdentityPool`.
  - A instalação da extensão **AADLoginForWindows** está bloqueada pela política do Azure.

- Para solucionar problemas de falhas de provisionamento da extensão **AADLoginForWindows**, você pode verificar os logs em `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` na máquina provisionada pelo MCS.

  > **Nota:**
  >
  > O MCS não depende da extensão `AADLoginForWindows` para unir uma VM ao Microsoft Entra ID ao usar uma imagem mestre com VDA versão 2209 ou posterior. Neste caso, a extensão `AADLoginForWindows` não será instalada na máquina provisionada pelo MCS. Portanto, os logs de provisionamento da extensão `AADLoginForWindows` não podem ser coletados.

- Verifique o status de junção do Microsoft Entra e os logs de depuração executando o comando `dsregcmd /status` na máquina provisionada pelo MCS.
- Verifique os logs de eventos do Windows em **Logs de Aplicativos e Serviços > Microsoft > Windows > Registro de Dispositivo de Usuário**.
- Verifique se o gerenciamento de dispositivos do Microsoft Entra está configurado corretamente executando `Get-Item -LiteralPath XDHyp:\Connections\${HostingConnectionName}`.

  Certifique-se de que o valor de:

  - a propriedade `AzureAdDeviceManagement` em `CustomProperties` seja **true**
  - a propriedade `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` nos metadados seja **true**

  Se `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` for **false**, isso indica que o `ServicePrincipal` do aplicativo usado pela conexão de hospedagem não tem permissões suficientes para realizar o gerenciamento de dispositivos do Microsoft Entra. Para resolver isso, atribua ao `ServicePrincipal` a função de **Administrador de Dispositivo na Nuvem**.

Grupos de segurança dinâmicos do Microsoft Entra

As regras de grupo dinâmico colocam as VMs no catálogo em um grupo de segurança dinâmico com base no esquema de nomenclatura do catálogo de máquinas.

Se o esquema de nomenclatura do catálogo de máquinas for Test### (onde # significa número), a Citrix® cria a regra de associação dinâmica \^*Test{3}$* no grupo de segurança dinâmico. Agora, se

o nome da VM criada pela Citrix for qualquer um de Test001 a Test999, a VM será incluída no grupo de segurança dinâmico.

Nota:

Se o nome da VM criada por você manualmente for qualquer um de Test001 a Test999, a VM também será incluída no grupo de segurança dinâmico. Esta é uma das limitações do grupo de segurança dinâmico.

O recurso de grupo de segurança dinâmico é útil quando você deseja gerenciar as VMs pelo Microsoft Entra ID. Isso também é útil quando você deseja aplicar políticas de Acesso Condicional ou distribuir aplicativos do Intune filtrando as VMs com o grupo de segurança dinâmico do Microsoft Entra.

Você pode usar comandos do **PowerShell** para:

- Criar um catálogo de máquinas com grupo de segurança dinâmico do Microsoft Entra
- Habilitar o recurso de grupo de segurança para um catálogo do Microsoft Entra
- Excluir um catálogo de máquinas com grupo de segurança de dispositivo unido ao Microsoft Entra

Importante:

- Para criar um catálogo de máquinas com grupo de segurança dinâmico do Microsoft Entra, adicionar máquinas ao catálogo e excluir o catálogo de máquinas, você deve ter um token de acesso do Microsoft Entra. Para obter informações sobre como obter o token de acesso do Microsoft Entra, consulte `<https://docs.microsoft.com/pt-br/graph/graph-explorer/graph-explorer-features#consent-to-permissions/>`.
- Para solicitar um token de acesso no Microsoft Entra ID, a Citrix solicita a permissão **Group.ReadWrite.All** para a API Microsoft Graph. Um usuário do Microsoft Entra que tenha permissão de consentimento de administrador em todo o locatário pode conceder a permissão **Group.ReadWrite.All** para a API Microsoft Graph. Para obter informações sobre como conceder consentimento de administrador em todo o locatário a um aplicativo no Microsoft Entra ID, consulte o documento da Microsoft `<https://`

`learn.microsoft.com/pt-br/entra/identity/enterprise-apps/grant-admin-consent>`.

- Você não precisa de um token de acesso do Microsoft Entra se usar uma conta de serviço do Microsoft Entra. Para obter informações sobre contas de serviço, consulte Contas de serviço para gerenciamento de identidade de máquina.

Criar um catálogo de máquinas com grupo de segurança dinâmico do Microsoft Entra

1. Na interface do usuário de configuração do catálogo de máquinas do console baseado na web, na página **Identidades da Máquina**, selecione **Unido ao Microsoft Entra**.
2. Faça login no Microsoft Entra ID.
3. Obtenha o token de acesso para a API MS Graph. Use este token de acesso como valor do parâmetro `$AzureADAccessToken` ao executar os comandos do **PowerShell**. Você não precisa de um token de acesso do Microsoft Entra se usar uma conta de serviço do Microsoft Entra.
4. Execute o seguinte comando para verificar se o nome do grupo de segurança dinâmico existe no locatário.

   ```
   Get-AcctAzureADSecurityGroup

   –AccessToken  $AzureADAccessToken

   –Name "SecurityGroupName"
   ```

   Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

   ```
   Get-AcctAzureADSecurityGroup -ServiceAccountUid <service account uid> –
   Name "SecurityGroupName"
   ```

5. Crie um catálogo de máquinas usando o ID do locatário, o token de acesso e o grupo de segurança dinâmico. Execute o seguinte comando para criar um IdentityPool com `IdentityType=AzureAD` e criar um grupo de segurança dinâmico no Azure.

   ```
   New-AcctIdentityPool

   -AllowUnicode
   ```

```
-IdentityPoolName "SecurityGroupCatalog"

-NamingScheme "SG-VM-###"

-NamingSchemeType "Numeric" -Scope @()

-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"

-WorkgroupMachine

-IdentityType "AzureAD"

-DeviceManagementType "None"

-AzureADTenantId  620387bb-9167-4bdd-8435-e3dccc58369e

-AzureADSecurityGroupName "SecurityGroupName"

-AzureADAccessToken $AzureADAccessToken
```

Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

```
New-AcctIdentityPool  -AllowUnicode -AzureADSecurityGroupName
"<security group name>" -AzureADTenantId "<Azure tenant id>"
-DeviceManagementType "Intune" -IdentityPoolName "dynamic security
group test" -IdentityType "AzureAD"  -NamingScheme "<naming scheme>"
-NamingSchemeType "Numeric" -Scope @() -ServiceAccountUid @("<service
account uid>") -StartCount 1 -WorkgroupMachine -ZoneUid "<Zone UID>"
```

Habilitar o recurso de grupo de segurança para um catálogo do Microsoft Entra

Você pode habilitar o recurso de segurança dinâmica para um catálogo do Microsoft Entra que foi criado sem o recurso de grupo de segurança dinâmica habilitado. Para fazer isso:

1. Crie manualmente um novo grupo de segurança dinâmico. Você também pode reutilizar um grupo de segurança dinâmico existente.
2. Faça login no Microsoft Entra ID e obtenha o token de acesso para a API MS Graph. Use este token de acesso como valor do parâmetro `$AzureADAccessToken` ao executar os comandos do **PowerShell**.

Nota:

- Para obter informações sobre as permissões exigidas pelo usuário do Microsoft Entra, consulte `<https://learn.microsoft.com/pt-br/entra/identity/enterprise-apps/grant-admin-consent?pivots=portal#prerequisites/>`.
- Você não precisa de um token de acesso do Microsoft Entra se usar uma conta de serviço do Microsoft Entra.

3. Execute o seguinte comando para conectar o pool de identidades ao grupo de segurança dinâmico do Microsoft Entra criado.

```
Set-AcctIdentityPool

-IdentityPoolName "SecurityGroupCatalog"

-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e

-AzureADSecurityGroupNam "ExistingSecurityGroupName"

-AzureADAccessToken $AzureADAccessToken
```

Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

```
Set-AcctIdentityPool

-IdentityPoolName "SecurityGroupCatalog"

-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e

-AzureADSecurityGroupNam "ExistingSecurityGroupName"

-ServiceAccountUid @("<service account uid>") -StartCount 1
-WorkgroupMachine -ZoneUid "<Zone UID>"
```

Se você atualizar o esquema de nomenclatura, o Citrix atualizará o esquema de nomenclatura para uma nova regra de associação. Se você excluir o catálogo, a regra de associação será excluída, e não o grupo de segurança.

Excluir um catálogo de máquinas com grupo de segurança de dispositivo associado ao Microsoft Entra

Ao excluir um catálogo de máquinas, o grupo de segurança de dispositivo associado ao Microsoft Entra também é excluído.

Para excluir o grupo de segurança dinâmico do Microsoft Entra, faça o seguinte:

1. Faça login no Microsoft Entra ID.
2. Obtenha o token de acesso para a API do MS Graph. Use este token de acesso como valor do parâmetro `$AzureADAccessToken` ao executar os comandos do **PowerShell**. Você não precisa de um token de acesso do Microsoft Entra se usar uma conta de serviço do Microsoft Entra.
3. Execute o seguinte comando:

   ```
   Remove-AcctIdentityPool

   -IdentityPoolName "SecurityGroupCatalog"

   -AzureADAccessToken $AzureADAccessToken
   ```

   Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

   ```
   Remove-AcctIdentityPool

   -IdentityPoolName "SecurityGroupCatalog"

   -ServiceAccountUid @("<service account uid>") -StartCount 1
   -WorkgroupMachine -ZoneUid "<Zone UID>"
   ```

Crie um grupo de segurança dinâmico do Microsoft Entra sob um grupo de segurança atribuído do Microsoft Entra ID existente

Você pode criar um grupo de segurança dinâmico do Microsoft Entra sob um grupo de segurança atribuído do Microsoft Entra ID existente. Você pode fazer o seguinte:

- Obtenha informações do grupo de segurança.
- Obtenha todos os grupos de segurança atribuídos do Microsoft Entra ID que são sincronizados de um servidor AD local ou os grupos de segurança atribuídos aos quais as funções do Microsoft Entra podem ser atribuídas.

- Obtenha todos os grupos de segurança dinâmicos do Microsoft Entra.
- Adicione o grupo de segurança dinâmico do Microsoft Entra como membro do grupo atribuído do Microsoft Entra ID.
- Remova a associação entre o grupo de segurança dinâmico do Microsoft Entra e o grupo de segurança atribuído do Microsoft Entra ID quando o grupo de segurança dinâmico do Microsoft Entra for excluído junto com o catálogo de máquinas.

Você também pode ver mensagens de erro explícitas quando qualquer uma das operações falhar.

Requisito:

Você deve ter o token de acesso para a API do MS Graph ao executar os comandos do **PowerShell**. Você não precisa de um token de acesso do Microsoft Entra se usar uma conta de serviço do Microsoft Entra. Portanto, em vez de `-AccessToken <token>`, use ServiceAccountUid `<service account uid>`.

Para obter o token de acesso:

1. Abra Microsoft graph explorer e faça login no Microsoft Entra ID.
2. Certifique-se de que você tenha consentimento para as permissões **Group.ReadWrite.All** e **GroupMember.ReadWrite.All**.
3. Obtenha o token de acesso do Microsoft graph explorer. Use este token de acesso ao executar os comandos **PowerShell**.

Para obter informações do grupo de segurança por ID do grupo:

1. Obtenha o token de acesso.
2. Encontre a ID do objeto do grupo no portal do Azure.
3. Execute o seguinte comando **PowerShell** no console do **PowerShell**:

   ```
   Get-AcctAzureADSecurityGroup

   -AccessToken <token> -GroupId <GroupUid>
   ```

   Ou, execute o seguinte se você estiver usando uma conta de serviço do Microsoft Entra:

   ```
   Get-AcctAzureADSecurityGroup -ServiceAccountUid <guid> -GroupId
   <GroupUid>
   ```

Para obter grupos de segurança pelo nome de exibição do grupo:

1. Obtenha o token de acesso.
2. Execute o seguinte comando **PowerShell** no console do **PowerShell**:

```
Get-AcctAzureADSecurityGroup

-AccessToken <token>

-Name <TargetGroupDisplayName>
```

   Ou, execute o seguinte se você estiver usando uma conta de serviço do Microsoft Entra:

```
Get-AcctAzureADSecurityGroup

-ServiceAccountUid <guid>

-Name <TargetGroupDisplayName>
```

Para obter grupos de segurança cujo nome de exibição contém uma substring:

1. Obtenha o token de acesso.
2. Execute o seguinte comando **PowerShell** no console do **PowerShell**:

```
Get-AcctAzureADSecurityGroup

-AccessToken <token>

-SearchString <displayNameSubString>
```

   Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

```
Get-AcctAzureADSecurityGroup

-ServiceAccountUid <guid>

-SearchString <displayNameSubString>
```

Para obter todos os grupos de segurança atribuídos ao Microsoft Entra ID que são sincronizados de um servidor AD local ou os grupos de segurança atribuídos aos quais as funções do Microsoft Entra podem ser atribuídas:

1. Obtenha o token de acesso.
2. Execute o seguinte comando **PowerShell** no console do **PowerShell**:

   ```
   Get-AcctAzureADSecurityGroup

   -AccessToken <token>

   -Assigned true
   ```

   Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

   ```
   Get-AcctAzureADSecurityGroup

   -ServiceAccountUid <guid>

   -Assigned true
   ```

Para obter todos os grupos de segurança dinâmicos do Microsoft Entra:

1. Obtenha o token de acesso.
2. Execute o seguinte comando **PowerShell** no console do **PowerShell**:

   ```
   Get-AcctAzureADSecurityGroup

   -AccessToken <token>

   -Dynamic true
   ```

   Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

   ```
   Get-AcctAzureADSecurityGroup

   -ServiceAccountUid <guid>

   -Dynamic true
   ```

Para obter grupos de segurança atribuídos ao Microsoft Entra ID com contagem máxima de registros:

1. Obtenha o token de acesso.
2. Execute o seguinte comando **PowerShell** no console do **PowerShell**:

```
Get-AcctAzureADSecurityGroup

-AccessToken <token>

-Assigned true

-MaxRecordCount 10
```

   Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

```
Get-AcctAzureADSecurityGroup

-ServiceAccountUid <guid>

-Assigned true

-MaxRecordCount 10
```

Para adicionar um grupo de segurança dinâmico do Microsoft Entra como membro de um grupo de segurança atribuído ao Microsoft Entra ID:

1. Obtenha o token de acesso.
2. Execute o seguinte comando **PowerShell** no console **PowerShell**:

```
Add-AcctAzureADSecurityGroupMember

-AccessToken <token>

-GroupId <ASG-Id>

-RefGroupId <DSG-Id>
```

   Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

```
Add-AcctAzureADSecurityGroupMember

-ServiceAccountUid <guid>

-GroupId <ASG-Id>

-RefGroupId <DSG-Id>
```

Para obter membros do grupo de segurança atribuído ao Microsoft Entra ID:

1. Obtenha o token de acesso.
2. Execute o seguinte comando **PowerShell** no console **PowerShell**:

```
Get-AcctAzureADSecurityGroupMember

-AccessToken <token>

-GroupId <ASG-Id>
```

Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

```
Get-AcctAzureADSecurityGroupMember

-ServiceAccountUid <guid>

-GroupId <ASG-Id>
```

Nota:

`Get-AcctAzureADSecurityGroupMember` fornece apenas os membros diretos do tipo de grupo de segurança sob o grupo de segurança atribuído ao Microsoft Entra ID.

Para remover a associação entre o grupo de segurança dinâmico do Microsoft Entra e o grupo de segurança atribuído ao Microsoft Entra ID quando o grupo de segurança dinâmico do Microsoft Entra é excluído junto com o catálogo de máquinas:

1. Obtenha o token de acesso.
2. Execute o seguinte comando **PowerShell** no console **PowerShell**:

```
Remove-AcctIdentityPool

-IdentityPoolName "SecurityGroupCatalog"

-AzureADAccessToken $AzureADAccessToken
```

Ou, execute o seguinte se estiver usando uma conta de serviço do Microsoft Entra:

```
Remove-AcctIdentityPool

-ServiceAccountUid <guid>

-IdentityPoolName "SecurityGroupCatalog"
```

Modificar nome do grupo de segurança dinâmico do Microsoft Entra

Você pode modificar o nome do grupo de segurança dinâmico do Microsoft Entra associado a um catálogo de máquinas. Essa modificação faz com que as informações do grupo de segurança armazenadas no objeto do pool de identidades do Microsoft Entra sejam consistentes com as informações armazenadas no portal do Azure.

Nota:

Os grupos de segurança dinâmicos do Microsoft Entra não incluem grupos de segurança sincronizados do AD local e outros tipos de grupo, como o grupo do Office 365.

Você pode modificar o nome do grupo de segurança dinâmico do Microsoft Entra usando comandos do Studio e do PowerShell.

Para modificar o nome do grupo de segurança dinâmico do Microsoft Entra usando o **PowerShell**:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos do **PowerShell** específicos da Citrix.
3. Execute o comando `Set-AcctIdentityPool -AzureAdSeurityGroupName [DSG-Name]`.

Você receberá mensagens de erro apropriadas se o nome do grupo de segurança dinâmico do Microsoft Entra não puder ser modificado.

Mais informações

- Contas de serviço para gerenciamento de identidade da máquina
- Contas de serviço do Microsoft Entra

Pool de identidades de identidade de máquina híbrida unida ao Microsoft Entra

Este artigo descreve como criar um pool de identidades de identidade de máquina híbrida unida ao Microsoft Entra usando o Citrix DaaS.

Para obter informações sobre requisitos, limitações e considerações, consulte Microsoft Entra híbrido unido.

Usar o Studio

As informações a seguir são um suplemento às orientações em Criar catálogos de máquinas. Para criar catálogos híbridos unidos ao Microsoft Entra, siga as orientações gerais desse artigo, atentando-se aos detalhes específicos dos catálogos híbridos unidos ao Microsoft Entra.

No assistente de criação de catálogo:

1. Na página **Identidades da Máquina**:
    a. Selecione o tipo de identidade como **Microsoft Entra híbrido unido**.
    b. Em Configurações avançadas, clique em **Selecionar conta de serviço** e selecione uma conta de serviço disponível na lista. Se uma conta de serviço adequada não estiver disponível para as identidades da máquina se unirem, você poderá criar uma conta de serviço. Para obter informações sobre contas de serviço, consulte Contas de serviço do Microsoft Entra.
    c. Clique em **Adicionar Atributos de Extensão** para armazenar dados exclusivos e personalizados diretamente nos objetos de dispositivo do Entra ID. Na página **Adicionar Atributos de Extensão**, adicione **Atributos de extensão** e **Valor**.

> **Nota:**
>
> - Você pode adicionar no máximo 15 atributos de extensão.
> - O nome e o valor devem ser únicos e não podem estar vazios.

d. Selecione uma opção de conta do Active Directory:

- **Criar novas contas do Active Directory**:
  - Se você selecionar **Criar novas contas do Active Directory** e usar um pool de identidades existente para criar novas contas, selecione um domínio para essas contas e especifique um esquema de nomenclatura de conta.
  - Se você selecionar **Criar novas contas do Active Directory** e usar um pool de identidades existente para criar novas contas, selecione um pool de identidades na lista.
- **Usar contas existentes do Active Directory**: Você pode procurar ou importar de um arquivo CSV e redefinir a senha ou especificar a mesma senha para todas as contas.

e. Clique em **Avançar**.

2. Na página **Credenciais de domínio**, selecione uma conta de serviço ou insira as credenciais manualmente. O pool de identidades híbrido do Microsoft Entra também pode ser associado a uma conta de serviço AD local. Para obter informações sobre contas de serviço, consulte Contas de serviço do Active Directory local.

Adicionar ou modificar atributos de extensão

Para alterar ou adicionar atributos de extensão adicionais a um catálogo de máquinas MCS existente, ou adicionar atributos de extensão a um catálogo MCS sem uma conta de serviço, use o assistente **Editar Catálogo de Máquinas**.

- Para alterar ou adicionar atributos de extensão adicionais, navegar até a página **Atributos de Extensão de Dispositivo do Microsoft Entra**. Clique no ícone de lápis e adicione ou atualize os atributos de extensão.
- Para adicionar atributos de extensão a um catálogo MCS sem uma conta de serviço do Microsoft Entra:

  a. navegar até a página **Conta de Serviço**. Selecione uma conta de serviço do Microsoft Entra para o Microsoft Intra ID.

  b. Vá para a página Atributos de Extensão de Dispositivo do Microsoft Entra, clique em **Adicionar Atributos de Extensão**.

Usar PowerShell

As seguintes etapas do PowerShell são equivalentes às operações no Studio.

A diferença entre catálogos unidos ao AD local e catálogos híbridos do Microsoft Entra reside na criação do pool de identidades e das contas de máquina.

Criar novo pool de identidades

Por exemplo: Para criar um pool de identidades junto com as contas para catálogos unidos ao Microsoft Entra híbrido:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

Nota:

O `$password` é a senha correspondente para uma conta de usuário do AD com Permissões de Gravação.

Todos os outros comandos usados para criar catálogos unidos ao Microsoft Entra híbrido são os mesmos que para catálogos tradicionais unidos ao AD local.

Você também pode associar uma conta de serviço local a um catálogo de máquinas criado pelo MCS, associando uma conta de serviço local ao pool de identidades. Você pode criar um pool de identidades ou atualizar um pool de identidades existente para associá-lo a uma conta de serviço.

Por exemplo: Para criar um novo pool de identidades e associá-lo a uma conta de serviço, execute o seguinte:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
```

```
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05" -ServiceAccountUid $serviceAccountUid
```

Por exemplo: Para criar um novo pool de identidades com atributos de extensão especificados e associá-lo a uma conta de serviço, execute o seguinte:

```
New-AcctIdentityPool -IdentityPoolName HybridAzureAD -NamingScheme ACC####
-NamingSchemeType Numeric -Domain "abc.local" -IdentityType HybridAzureAD
-ServiceAccountUid $serviceAccountUid -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

Quando uma VM é ligada pela primeira vez, após ingressar no Microsoft Entra ID, a VM reporta seu deviceId do Entra ID ao MCS.

Por exemplo: Para verificar o `EntraIDDeviceID`, execute `Get-AcctADAccount` ou `Get-AcctIdentity`.

```
Get-AcctADAccount -IdentityPoolName MyPool
```

Após a reinicialização, para VMs persistentes e não persistentes, o `EntraIDDeviceID` permanece o mesmo.

> **Nota:**
>
> O MCS remove automaticamente os IDs de dispositivo associados e os atributos de extensão quando você exclui uma VM do catálogo, mas não a exclui do Azure.

Atualizar pool de identidades existente

Por exemplo: Para atualizar um pool de identidades existente para associá-lo a uma conta de serviço, execute o seguinte:

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid
```

```
Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid -ServiceAccountUid
$serviceAccountUid
```

Nota:

O `$serviceAccountUid` deve ser um UID válido de uma conta de serviço do Active Directory local.

Por exemplo: Para editar atributos de extensão para o catálogo existente, execute o seguinte:

Nota:

- Após atualizar as VMs do catálogo existente para a versão 2511 ou posterior do VDA, é necessário reiniciar. Essa reinicialização permite que a VM relate seu deviceId do Entra ID ao MCS, permitindo que o MCS configure os atributos de extensão da VM.
- O catálogo existente deve ter uma conta de serviço do tipo AzureAD com a permissão "Device.ReadWrite.All".

Para adicionar novos atributos:

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

Para remover alguns atributos existentes

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{}
```

OU

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{extensionAttribute1 = ""; extensionAttribute2 = ""}
```

`Set-AcctIdentityPool` também atualiza os atributos de extensão do dispositivo Entra ID para VMs que já estão unidas ao Entra ID e possuem um valor `EntraIDDeviceID` em suas identidades.

Criar um catálogo híbrido do Microsoft Entra

Você também pode criar um catálogo híbrido do Microsoft Entra usando uma imagem preparada. Para o conjunto completo de comandos do PowerShell para criar a definição de imagem, a versão da imagem e a especificação da versão da imagem preparada, consulte:

- Ambiente de virtualização do Azure: Usar PowerShell.
- Ambiente de virtualização VMware: Usar PowerShell

Após criar a especificação da versão da imagem preparada, crie o pool de identidades e o catálogo de máquinas. Por exemplo:

```
New-AcctIdentityPool -IdentityPoolName "mypool" -NamingScheme ACC##  -
NamingSchemeType "Numeric"  -ZoneUid $zoneuid -Domain $domainName -OU
"OU=HAAD Computers,DC=haad,DC=link" -IdentityType "HybridAzureAD"



New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
<preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid> -IdentityPoolUid
<IdentityPoolUid> [-CleanOnBoot] -NetworkMapping @{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.folder
\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<sunNetN
ame>.network"} -ServiceOffering <serviceofferingPath> [-MachineProfile
<machineProfilePath>] [-CustomProperties <>]
```

Visualizar o status do processo de junção híbrida do Microsoft Entra

No Studio, o status do processo de junção híbrida do Microsoft Entra é visível quando as máquinas unidas hibridamente ao Microsoft Entra em um grupo de entrega estão em estado ligado. Para visualizar o status, use Pesquisar para identificar essas máquinas e, em seguida, para cada uma, verifique **Identidade da Máquina** na guia **Detalhes** no painel inferior. As seguintes informações podem aparecer em **Identidade da Máquina**:

- Unido hibridamente ao Microsoft Entra
- Ainda não unido ao Microsoft Entra ID

> **Nota:**
>
> - Você pode experimentar um atraso na junção híbrida do Microsoft Entra quando a máquina é ligada inicialmente. Isso é causado pelo intervalo de sincronização padrão da identidade da máquina (30 minutos do Microsoft Entra Connect). A máquina estará no estado de junção híbrida do Microsoft Entra somente depois que as identidades da máquina forem sincronizadas com o Microsoft Entra ID através do Microsoft Entra Connect.
> - Se as máquinas não conseguirem entrar no estado de junção híbrida do Microsoft Entra, elas não serão registradas no Delivery Controller. O status de registro delas aparece como **Inicialização**.

> Além disso, usando o Studio, você pode descobrir por que as máquinas estão indisponíveis. Para fazer isso, clique em uma máquina no nó **Pesquisar**, verifique **Registro** na guia **Detalhes** no painel inferior e, em seguida, leia a dica de ferramenta para obter informações adicionais.

Solução de problemas

Se as máquinas não conseguirem ser unidas hibridamente ao Microsoft Entra, faça o seguinte:

- Verifique se a conta da máquina foi sincronizada com o Microsoft Entra ID através do portal Microsoft Microsoft Entra. Se sincronizada, **Ainda não unido ao Microsoft Entra ID** aparece, indicando status de registro pendente.

  Para sincronizar contas de máquina com o Microsoft Entra ID, certifique-se de que:

  - A conta da máquina está na UO configurada para ser sincronizada com o Microsoft Entra ID. Contas de máquina sem o atributo **userCertificate** não são sincronizadas com o Microsoft Entra ID, mesmo que estejam na UO configurada para ser sincronizada.
  - O atributo **userCertificate** é preenchido na conta da máquina. Use o Active Directory Explorer para visualizar o atributo.
  - O Microsoft Entra Connect deve ter sido sincronizado pelo menos uma vez após a criação da conta da máquina. Caso contrário, execute manualmente o comando `Start-`

`ADSyncSyncCycle -PolicyType Delta` no console do PowerShell da máquina do Microsoft Entra Connect para acionar uma sincronização imediata.

- Verifique se o par de chaves do dispositivo gerenciado pelo Citrix para junção híbrida do Microsoft Entra foi corretamente enviado para a máquina, consultando o valor de **DeviceKeyPairRestored** em **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**.

  Verifique se o valor é 1. Caso contrário, as possíveis razões são:

  - `IdentityType` do pool de identidades associado ao esquema de provisionamento não está definido como `HybridAzureAD`. Você pode verificar isso executando `Get-AcctIdentityPool`.
  - A máquina não foi provisionada usando o mesmo esquema de provisionamento do catálogo de máquinas.
  - A máquina não está ingressada no domínio local. O ingresso no domínio local é um pré-requisito para o ingresso híbrido no Microsoft Entra.

- Verifique as mensagens de diagnóstico executando o comando `dsregcmd /status /debug` na máquina provisionada pelo MCS.

  - Se o ingresso híbrido no Microsoft Entra for bem-sucedido, **AzureAdJoined** e **DomainJoined** serão **SIM** na saída da linha de comando.
  - Caso contrário, consulte a documentação da Microsoft para solucionar os problemas: `<https://docs.microsoft.com/pt-br/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`.
  - Se você receber a mensagem de erro **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**, execute o seguinte comando PowerShell para reparar o certificado do usuário:

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
    UserCertificate
    ```

Para obter mais informações sobre o problema do certificado do usuário, consulte CTX566696.

Pool de identidades de identidade de máquina habilitada para Microsoft Intune

Este artigo descreve como criar um pool de identidades de identidade de máquina habilitada para Microsoft Intune usando o Citrix DaaS.

Você pode criar:

- Catálogos unidos ao Microsoft Entra inscritos no Microsoft Intune para VMs persistentes e não persistentes, de sessão única e multi-sessão. Para criar catálogos, consulte Criar catálogos unidos ao Microsoft Entra inscritos no Microsoft Intune.
- Catálogos híbridos unidos ao Microsoft Entra inscritos no Microsoft Intune para VMs persistentes de sessão única e multi-sessão usando credencial de dispositivo com capacidade de cogestão. Para criar catálogos, consulte Criar catálogos híbridos unidos ao Microsoft Entra inscritos no Microsoft Intune. Você também pode criar catálogos híbridos unidos ao Microsoft Entra inscritos no Microsoft Intune para VMs não persistentes de sessão única e multi-sessão. No entanto, isso está atualmente em Pré-visualização. Consulte Inscrição de VMs não persistentes unidas ao Hybrid Entra ID no Microsoft Intune.

Para obter informações sobre requisitos, limitações e considerações, consulte Microsoft Intune.

Criar catálogos unidos ao Microsoft Entra inscritos no Microsoft Intune

Você pode criar catálogos unidos ao Microsoft Entra inscritos no Microsoft Intune para VMs persistentes e não persistentes usando o Studio e o PowerShell.

Para obter informações sobre requisitos, limitações e considerações, consulte:

- Requisitos para catálogos unidos ao Microsoft Entra inscritos no Microsoft Intune
- Limitações para catálogos unidos ao Microsoft Entra inscritos no Microsoft Intune

Usar o Studio

As informações a seguir são um complemento às orientações em Criar catálogos de máquinas.

No assistente de criação de catálogo:

- Na página **Identidades da Máquina**:
  - Selecione **Microsoft Entra joined** e depois **Registrar as máquinas no Microsoft Intune**. Se ativado, registre as máquinas no Microsoft Intune para gerenciamento. Você pode criar catálogos unidos ao Microsoft Entra registrados no Microsoft Intune para VMs persistentes

e não persistentes de sessão única e multi-sessão. No entanto, para VMs não persistentes, você deve ter a versão do VDA 2407 ou posterior.

- Clique em **Selecionar conta de serviço** e selecione uma conta de serviço disponível na lista. Se uma conta de serviço adequada não estiver disponível para o locatário do Microsoft Entra ao qual as identidades da máquina se juntarão, você poderá criar uma conta de serviço. Para obter informações sobre contas de serviço, consulte Contas de serviço do Microsoft Entra.

  > **Nota:**
  >
  > A conta de serviço que você selecionou pode estar em um status não saudável devido a várias razões. Você pode ir para **Administradores > Contas de Serviço** para visualizar detalhes e corrigir os problemas de acordo com as recomendações. Alternativamente, você pode prosseguir com a operação do catálogo de máquinas e corrigir os problemas mais tarde. Se você não corrigir o problema, dispositivos unidos ao Microsoft Entra ou registrados no Microsoft Intune obsoletos serão gerados, o que pode bloquear a união das máquinas ao Microsoft Entra.

- Clique em **Adicionar Atributos de Extensão** para armazenar dados exclusivos e personalizados diretamente em seus objetos de dispositivo do Entra ID. Na página **Adicionar Atributos de Extensão**, adicione **Atributos de extensão** e **Valor**.

  > **Nota:**
  >
  > - Você pode adicionar um máximo de 15 atributos de extensão.
  > - O nome e o valor devem ser únicos e não podem estar vazios.

Adicionar ou modificar atributos de extensão

Para alterar ou adicionar atributos de extensão adicionais a um catálogo de máquinas MCS existente, ou adicionar atributos de extensão a um catálogo MCS sem uma conta de serviço, use o assistente **Editar Catálogo de Máquinas**.

- Para alterar ou adicionar atributos de extensão adicionais, navegar para a página **Atributos de Extensão de Dispositivo do Microsoft Entra**. Clique no ícone de lápis e adicione ou atualize os atributos de extensão.

- Para adicionar atributos de extensão a um catálogo MCS sem uma conta de serviço do Microsoft Entra:

  a. navegar para a página **Conta de Serviço**. Selecione uma conta de serviço do Microsoft Entra para o Microsoft Intra ID.

  b. Vá para a página Atributos de Extensão de Dispositivo do Microsoft Entra, clique em **Adicionar Atributos de Extensão**.

Usar PowerShell

A seguir estão as etapas do PowerShell que são equivalentes às operações no Studio.

Para registrar máquinas no Microsoft Intune usando o SDK do PowerShell Remoto, use o parâmetro `DeviceManagementType` em `New-AcctIdentityPool`. Este recurso exige que o catálogo esteja associado ao Microsoft Entra e que o Microsoft Entra ID possua a licença correta do Microsoft Intune. Por exemplo:

```
New-AcctIdentityPool -AllowUnicode -DeviceManagementType "Intune"
IdentityType="AzureAD" -WorkgroupMachine -IdentityPoolName
"AzureADJoinedCatalog" -NamingScheme "AzureAD-VM-##" -NamingSchemeType
"Numeric" -ServiceAccountUid $serviceAccountUid -Scope @() -ZoneUid
"81291221-d2f2-49d2-ab12-bae5bbd0df05"
```

Por exemplo: Para criar um novo pool de identidades com atributos de extensão especificados e associá-lo a uma conta de serviço, execute o seguinte:

```
New-AcctIdentityPool -IdentityPoolName MyPool -NamingScheme ACC####
-NamingSchemeType Numeric -Domain "abc.local" -IdentityType AzureAD
-ServiceAccountUid $serviceAccountUid -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

Quando uma VM é ligada pela primeira vez, após ingressar no Microsoft Entra ID, a VM reporta seu deviceId do Entra ID ao MCS.

Por exemplo: Para verificar o `EntraIDDeviceID`, execute `Get-AcctADAccount` ou `Get-AcctIdentity`.

```
Get-AcctADAccount -IdentityPoolName MyPool
```

Após a reinicialização, para VMs persistentes, o `EntraIDDeviceID` permanece o mesmo. Para VMs não persistentes, há um novo `EntraIDDeviceID` após cada reinicialização.

> **Nota:**

> O MCS remove automaticamente os atributos de extensão associados quando você exclui uma VM do catálogo, mas não a exclui do Azure.

> Por exemplo: Para editar atributos de extensão para o catálogo existente, execute o seguinte:

> **Nota:**

> - Após atualizar as VMs do catálogo existente para a versão 2511 ou posterior do VDA, é necessária uma reinicialização. Essa reinicialização permite que a VM reporte seu deviceId do Entra ID ao MCS, permitindo que o MCS configure os atributos de extensão da VM.
> - O catálogo existente deve ter uma conta de serviço do tipo AzureAD com a permissão "Device.ReadWrite.All".

> Para adicionar novos atributos:

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

Para remover alguns atributos existentes

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{}
```

OU

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{extensionAttribute1 = ""; extensionAttribute2 = ""}
```

`Set-AcctIdentityPool` também atualiza os atributos de extensão do dispositivo Entra ID para VMs que já estão unidas ao Entra ID e possuem um valor `EntraIDDeviceID` em suas identidades.

Por exemplo: Para criar um catálogo do Microsoft Entra inscrito no Microsoft Intune usando uma imagem preparada:

```
New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
<preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid> -IdentityPoolUid
<IdentityPoolUid> [-CleanOnBoot] -NetworkMapping @{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.folder
\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<sunNetN
ame>.network"} -ServiceOffering <serviceofferingPath> [-MachineProfile
<machineProfilePath>] [-CustomProperties <>]
```

Solução de problemas

Se as máquinas falharem ao se inscrever no Microsoft Intune, faça o seguinte:

- Verifique se as máquinas provisionadas pelo MCS estão unidas ao Microsoft Entra. As máquinas falham ao se inscrever no Microsoft Intune se não estiverem unidas ao Microsoft Entra. Consulte Solução de problemas para solucionar problemas de junção ao Microsoft Entra.
- Verifique se o seu locatário do Microsoft Entra está atribuído com a licença Intune apropriada. Consulte `<https://learn.microsoft.com/pt-br/mem/intune/fundamentals/licenses>` para os requisitos de licença do Microsoft Intune.
- Para catálogos que usam imagens mestras com VDA versão 2206 ou anterior, verifique o status de provisionamento da extensão **AADLoginForWindows** para as máquinas. Se a extensão **AADLoginForWindows** não existir, as possíveis razões são:
  - `IdentityType` do pool de identidades associado ao esquema de provisionamento não está definido como `AzureAD` ou `DeviceManagementType` não está definido como `Intune`. Você pode verificar isso executando `Get-AcctIdentityPool`.
  - A política do Azure bloqueou a instalação da extensão **AADLoginForWindows**.
- Para solucionar falhas de provisionamento da extensão **AADLoginForWindows**, você pode verificar os logs em `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` na máquina provisionada pelo MCS.

> **Nota:**
>
> O MCS não depende da extensão `AADLoginForWindows` para unir uma VM ao Microsoft Entra ID e se inscrever no Microsoft Intune ao usar uma imagem mestra com VDA versão 2209 ou posterior. Neste caso, a extensão `AADLoginForWindows` não é instalada na máquina provisionada pelo MCS. Portanto, os logs de provisionamento da extensão `AADLoginForWindows` não podem ser coletados.

- Verifique os logs de eventos do Windows em **Logs de Aplicativos e Serviços > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider**.
- A conta de serviço que você selecionou pode estar em um status não saudável devido a várias razões. Você pode ir para **Administradores > Contas de Serviço** para ver detalhes e corrigir os problemas de acordo com as recomendações. Se você não corrigir o problema, dispositivos unidos ao Microsoft Entra ou inscritos no Microsoft Intune obsoletos serão gerados, o que pode bloquear a junção ao Microsoft Entra das máquinas.

Criar catálogos híbridos unidos ao Microsoft Entra inscritos no Microsoft Intune

Você pode criar catálogos habilitados para cogestão para catálogos ingressados no Microsoft Entra híbrido registrados no Microsoft Intune para VMs persistentes de sessão única e multi-sessão. Você pode criar catálogos habilitados para cogestão usando o Studio e o PowerShell.

Para obter informações sobre requisitos, limitações e considerações, consulte:

- Requisitos para catálogos ingressados no Microsoft Entra híbrido registrados no Microsoft Intune
- Limitações para catálogos ingressados no Microsoft Entra híbrido registrados no Microsoft Intune

Usar o Studio

As informações a seguir são um complemento às orientações em Criar catálogos de máquinas.

No assistente de **Configuração do Catálogo de Máquinas**:

- Na página **Identidades da Máquina**, selecione **Ingressado no Microsoft Entra híbrido** e, em seguida, **Registrar as máquinas no Microsoft Intune com o Configuration Manager**. Com esta ação, o Configuration Manager e o Microsoft Intune (ou seja, cogestionados) gerenciam as VMs.

- Clique em **Adicionar Atributos de Extensão** para armazenar dados exclusivos e personalizados diretamente nos objetos de dispositivo do Entra ID. Na página **Adicionar Atributos de Extensão**, adicione **Atributos de extensão** e **Valor**.

  > **Nota:**
  >
  > - Você pode adicionar um máximo de 15 atributos de extensão.
  > - O nome e o valor devem ser únicos e não podem estar vazios.

Adicionar ou modificar atributos de extensão

Para alterar ou adicionar atributos de extensão adicionais a um catálogo de máquinas MCS existente, ou adicionar atributos de extensão a um catálogo MCS sem uma conta de serviço, use o assistente **Editar Catálogo de Máquinas**.

- Para alterar ou adicionar atributos de extensão adicionais, navegar para a página **Atributos de Extensão de Dispositivo do Microsoft Entra**. Clique no ícone de lápis e adicione ou atualize os atributos de extensão.
- Para adicionar atributos de extensão a um catálogo MCS sem uma conta de serviço do Microsoft Entra:

  a. navegar para a página **Conta de Serviço**. Selecione uma conta de serviço do Microsoft Entra para o Microsoft Intra ID.

  b. Vá para a página Atributos de Extensão de Dispositivo do Microsoft Entra, clique em **Adicionar Atributos de Extensão**.

Usar PowerShell

A seguir estão as etapas do PowerShell equivalentes às etapas no Studio.

Para registrar máquinas no Microsoft Intune com o Configuration Manager usando o SDK do PowerShell Remoto, use o parâmetro `DeviceManagementType` em `New-AcctIdentityPool`. Este recurso exige que o catálogo seja ingressado no Microsoft Entra híbrido e que o Microsoft Entra ID possua a licença correta do Microsoft Intune.

A diferença entre catálogos ingressados no Microsoft Entra híbrido e os habilitados para cogestão reside na criação do pool de identidades. Por exemplo:

```
New-AcctIdentityPool -AllowUnicode -DeviceManagementType "IntuneWithSCCM"
IdentityType="HybridAzureAD" -IdentityPoolName "CoManagedCatalog"
-NamingScheme "CoManaged-VM-##" -NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
```

Por exemplo: Para criar um novo pool de identidades com atributos de extensão especificados e associá-lo a uma conta de serviço, execute o seguinte:

```
New-AcctIdentityPool -IdentityPoolName HybridAzureAD -NamingScheme ACC####
-NamingSchemeType Numeric -Domain "abc.local" -IdentityType HybridAzureAD
-ServiceAccountUid $serviceAccountUid -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

Quando uma VM é ligada pela primeira vez, após ingressar no Microsoft Entra ID, a VM reporta seu deviceId do Entra ID ao MCS.

Por exemplo: Para verificar o `EntraIDDeviceID`, execute `Get-AcctADAccount` ou `Get-AcctIdentity`.

```
Get-AcctADAccount -IdentityPoolName MyPool
```

Após a reinicialização, para VMs persistentes e não persistentes, o `EntraIDDeviceID` permanece o mesmo.

Nota:

O MCS remove automaticamente os IDs de dispositivo e atributos de extensão associados quando você exclui uma VM do catálogo, mas não a exclui do Azure.

Por exemplo: Para editar atributos de extensão para o catálogo existente, execute o seguinte:

Nota:

- Após atualizar as VMs de catálogo existentes para a versão VDA 2511 ou posterior, é necessário reiniciar. Essa reinicialização permite que a VM relate seu deviceId do Entra ID ao MCS, permitindo que o MCS configure os atributos de extensão da VM.
- O catálogo existente deve ter uma conta de serviço do tipo AzureAD com a permissão "Device.ReadWrite.All".

Para adicionar novos atributos:

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{"extensionAttribute1" = "val1"; "extensionAttribute2" = "val2"}
```

Para remover alguns atributos existentes

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{}
```

OU

```
Set-AcctIdentityPool -IdentityPoolName MyPool -EntraIDExtensionAttributes
@{extensionAttribute1 = ""; extensionAttribute2 = ""}
```

`Set-AcctIdentityPool` também atualiza os atributos de extensão do dispositivo Entra ID para VMs que já estão unidas ao Entra ID e possuem um valor `EntraIDDeviceID` em suas identidades.

Você também pode criar um catálogo persistente Híbrido do Microsoft Entra inscrito no Microsoft Intune usando uma imagem preparada. Para o conjunto completo de comandos do PowerShell para criar a definição de imagem, a versão da imagem e a especificação da versão da imagem preparada, consulte:

- Ambiente de virtualização do Azure: Usar PowerShell.
- Ambiente de virtualização VMware: Usar PowerShell

Após criar a especificação da versão da imagem preparada, crie o pool de identidades e o catálogo de máquinas. Por exemplo:

```
New-AcctIdentityPool -IdentityPoolName "mypool" -NamingScheme ACC##  -
NamingSchemeType "Numeric"  -ZoneUid $zoneuid -Domain $domainName -OU
"OU=HAAD Computers,DC=haad,DC=link" -IdentityType "HybridAzureAD"
-DeviceManagement IntuneWithSCCM



New-ProvScheme -ProvisioningSchemeName <name> -ImageVersionSpecUid
<preparedVersionSpecUid> -HostingUnitUid <hostingUnitUid> -IdentityPoolUid
<IdentityPoolUid> [-CleanOnBoot] -NetworkMapping @{"0"="XDHyp:
\HostingUnits\<hostingunitName>\<region>.region\virtualprivatecloud.folder
\<resourcegroupName>.resourcegroup\<vnetName>.virtualprivatecloud\<sunNetN
ame>.network"} -ServiceOffering <serviceofferingPath> [-MachineProfile
<machineProfilePath>] [-CustomProperties <>]
```

Nota:

A inscrição de VMs não persistentes unidas ao Microsoft Entra híbrido no Microsoft Intune está atualmente em visualização.

Solução de problemas

Se as máquinas falharem ao se inscrever no Microsoft Intune ou falharem ao atingir o estado de cogestão, faça o seguinte:

- Verificar licença do Intune

  Verifique se o seu locatário do Microsoft Entra está atribuído com a licença Intune apropriada. Consulte Licenciamento do Microsoft Intune para os requisitos de licença do Microsoft Intune.

- Verificar o status de ingresso híbrido do Microsoft Entra

  Verifique se as máquinas provisionadas pelo MCS estão ingressadas no Microsoft Entra híbrido. As máquinas não são elegíveis para co-gerenciamento se não estiverem ingressadas no Microsoft Entra híbrido. Consulte Solução de problemas para solucionar problemas de ingresso híbrido do Microsoft Entra.

- Verificar a elegibilidade para co-gerenciamento

- Verifique se as máquinas provisionadas pelo MCS estão corretamente atribuídas ao site esperado do Configuration Manager. Para obter o site atribuído, execute o seguinte comando PowerShell nas máquinas afetadas.

  ```
  (New-Object -ComObject "Microsoft.SMS.Client").GetAssignedSite()
  ```

- Se nenhum site estiver atribuído à VM, use o seguinte comando para verificar se o site do Configuration Manager pode ser descoberto automaticamente.

  ```
  (New-Object -ComObject "Microsoft.SMS.Client").AutoDiscoverSite()
  ```

- Certifique-se de que os limites e grupos de limites estejam bem configurados em seu ambiente do Configuration Manager se nenhum código de site puder ser descoberto. Consulte Considerações para obter detalhes.
- Verifique `C:\Windows\CCM\Logs\ClientLocation.log` para quaisquer problemas de atribuição de site do cliente do Configuration Manager.
- Verifique os estados de co-gerenciamento das máquinas. Abra o **painel de controle do Configuration Manager** nas máquinas afetadas e vá para a guia **Geral**. O valor da propriedade Co-management deve ser **Habilitado**. Caso contrário, verifique os logs em `C:\Windows\CCM\Logs\CoManagementHandler.log`.

- Verificar o registro no Intune

  As máquinas podem falhar ao se registrar no Microsoft Intune mesmo que todos os pré-requisitos sejam satisfeitos. Verifique os logs de eventos do Windows em **Logs de Aplicativos e Serviços > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider** para problemas de registro no Intune.

Mais informações

- Contas de serviço para gerenciamento de identidade de máquina
- Contas de serviço do Microsoft Entra

Pool de identidade de máquina não associada a domínio

Este artigo descreve como criar um pool de identidade de máquina não associada a domínio usando o Citrix DaaS.

Para obter informações sobre requisitos, limitações e considerações, consulte Não associado a domínio.

Antes de criar o catálogo de máquinas, você precisa do seguinte:

1. Novo local de recurso
    - navegar para a interface de usuário de administração do Citrix Cloud™ > menu hambúrguer superior esquerdo > **Resource Locations**.
    - Clique em **+ Resource Location**.
    - Insira um nome para o novo local de recurso e clique em **Save**.
2. Crie uma conexão de hospedagem. Consulte a seção Criar e gerenciar conexões para obter detalhes.

Usando o Citrix DaaS, você pode criar catálogos baseados em grupos de trabalho para máquinas não associadas a domínio. A criação de máquinas não associadas a domínio depende de como o pool de identidade da conta é criado. O pool de identidade da conta é o mecanismo usado pelo MCS para criar e rastrear nomes de máquinas durante o provisionamento do catálogo.

Você pode criar catálogos não associados a domínio usando o Studio ou o PowerShell.

Usar o Studio

As informações a seguir são um complemento às orientações em Criar catálogos de máquinas. Para criar catálogos não associados a domínio, siga as orientações gerais desse artigo, observando os detalhes específicos dos catálogos não associados a domínio.

No assistente de criação de catálogo:

- Na página **Machine Identities**, selecione **Non-domain-joined**. As máquinas criadas não estão associadas a nenhum domínio.

> **Nota:**
>
> O tipo de identidade **Não-associado ao domínio** requer a versão 1811 ou posterior do VDA como nível funcional mínimo para o catálogo. Para torná-lo disponível, atualize o nível funcional mínimo, se necessário.

Usar PowerShell

A seguir estão as etapas do PowerShell equivalentes às operações no Studio.

Você pode criar um pool de identidades para catálogos não associados ao domínio usando o SDK do PowerShell Remoto.

Use os parâmetros do PowerShell, **WorkgroupMachine** e **IdentityType**, para criar um pool de identidades para catálogos não associados ao domínio. Os parâmetros eliminam a necessidade de especificar todos os parâmetros específicos do AD, incluindo as credenciais de administrador de domínio:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

Todos os outros comandos usados para criar catálogos não associados ao domínio são os mesmos que para os catálogos tradicionais associados ao Active Directory no local.

Gerenciar catálogos de máquinas

Nota:

Este artigo descreve como gerenciar catálogos usando comandos do Studio e do PowerShell. Se você criou o catálogo usando o nó Quick Deploy e continua usando esse nó para gerenciar o catálogo, siga Gerenciar catálogos no Quick Deploy.

Introdução

Você pode adicionar ou remover máquinas de um catálogo de máquinas, e renomear, alterar a descrição ou gerenciar as contas de computador do Active Directory de um catálogo.

A manutenção do catálogo também pode incluir as tarefas de garantir que cada máquina tenha as atualizações mais recentes do sistema operacional, atualizações de software antivírus, atualizações do sistema operacional ou alterações de configuração.

- Catálogos contendo máquinas aleatórias agrupadas criadas usando Machine Creation Services™ (MCS) mantêm as máquinas atualizando a imagem usada no catálogo e, em

seguida, atualizando as máquinas. Este método permite atualizar um grande número de máquinas de usuário de forma eficiente.

- Para catálogos contendo máquinas estáticas e permanentemente atribuídas, você pode gerenciar a imagem ou o modelo que esses catálogos usam atualmente, mas apenas as máquinas que você adicionar aos catálogos posteriormente serão criadas usando a nova imagem ou modelo.
- Para catálogos de Acesso Remoto a PC, você gerencia as atualizações das máquinas dos usuários fora do Studio. Execute esta tarefa individualmente ou coletivamente usando ferramentas de distribuição de software de terceiros.

Para obter informações sobre como criar e gerenciar conexões com hipervisores de host e serviços de nuvem, consulte Criar e gerenciar conexões e recursos.

> **Nota:**
>
> O MCS não oferece suporte ao Windows 10 IoT Core e ao Windows 10 IoT Enterprise. Consulte o site da Microsoft para obter mais informações.

Sobre instâncias persistentes

Ao atualizar a imagem mestre para um catálogo MCS contendo máquinas persistentes, quaisquer novas máquinas adicionadas ao catálogo usarão a imagem atualizada. As máquinas existentes continuarão a usar a imagem mestre original. O processo de atualização de uma imagem é feito da mesma forma para qualquer outro tipo de catálogo. Considere o seguinte:

- Com catálogos de disco persistentes, as máquinas pré-existentes não são atualizadas para a nova imagem, mas quaisquer novas máquinas adicionadas ao catálogo usam a nova imagem.
- Para catálogos de disco não persistentes, a imagem da máquina é atualizada na próxima vez somente se a máquina for reiniciada dentro do Studio ou PowerShell. Se a máquina for reiniciada do hipervisor fora do Studio, o disco não será redefinido.
- Para catálogos que não persistem, se você quiser imagens diferentes para máquinas diferentes, as imagens devem residir em catálogos separados.

Gerenciar Catálogos de Máquinas

Você pode gerenciar um catálogo de máquinas de duas maneiras:

- Usando o Studio

- Usando o PowerShell

Usar o Studio

Esta seção detalha como você pode gerenciar catálogos usando o Studio:

- Exibir detalhes do catálogo
- Adicionar máquinas a um catálogo
- Excluir máquinas de um catálogo
- Editar um catálogo
- Renomear um catálogo
- Excluir um catálogo
- Gerenciar contas de computador do Active Directory em um catálogo
- Alterar a imagem mestre para um catálogo
- Converter catálogos provisionados por MCS de imagens mestre para imagens preparadas.
- Alterar o nível funcional ou desfazer a alteração
- Clonar um catálogo
- Organizar catálogos usando pastas
- Atualizar VDAs
- Gerenciar configurações de otimização de experiência para um catálogo
- Tentar novamente a criação do catálogo
- (Somente VDAs não provisionados pelo Citrix®) Gerar e gerenciar tokens de registro

Exibir detalhes do catálogo

1. Use a função de pesquisa para localizar um catálogo de máquinas específico. Consulte Pesquisar instâncias para obter instruções.
2. Nos resultados da pesquisa, selecione um catálogo conforme necessário.
3. Consulte a tabela a seguir para obter descrições das colunas do catálogo.

COLUNA	DESCRIÇÃO
Catálogo de Máquinas	O nome e o tipo de alocação do catálogo. Os tipos de alocação incluem

COLUNA	DESCRIÇÃO
	• Aleatório: As máquinas no catálogo são alocadas a um usuário aleatoriamente.
	• Permanente: As máquinas no catálogo são alocadas a um usuário permanentemente.
Tipo de Máquina	O tipo de sessão suportado das máquinas no catálogo. Os valores possíveis incluem
	• Tipo de SO: SO multi-sessão (Virtual); Dados do usuário: Descartar.
	• Tipo de SO: SO multi-sessão (Virtual); Dados do usuário: No disco local
	• Tipo de SO: SO de sessão única (Acesso Remoto a PC)
	• Tipo de SO: SO de sessão única (Virtual); Dados do usuário: Descartar
	• Tipo de SO: SO de sessão única (Virtual); Dados do usuário: No disco local
Contagem de Máquinas	A contagem de máquinas no catálogo e o método de provisionamento. Os métodos de provisionamento possíveis incluem: Machine Creation Services (máquina MCS), Manual e Citrix Provisioning™ Services.
Contagem Alocada	O número de máquinas no catálogo atribuídas a um grupo de entrega.
Pasta	O local do catálogo na árvore de **Catálogos de Máquinas**. Ele exibe o nome da pasta em que o catálogo está (incluindo a barra invertida final), ou `-` se o catálogo estiver no nível raiz.

COLUNA	DESCRIÇÃO
Atualização do VDA	Estado da Atualização do VDA. Os valores possíveis incluem: Não configurado, Agendado, Disponível e Atualizado.
Status da Imagem	O status da atualização da imagem do catálogo. Aplicável apenas a catálogos de máquinas não persistentes. Os valores possíveis incluem: Totalmente atualizado, Parcialmente atualizado, Atualizações pendentes, Preparando

4. Clique em uma guia no painel de detalhes inferior para obter mais informações sobre um catálogo selecionado.

GUIA	DESCRIÇÃO
Detalhes	Resume as principais configurações do catálogo de máquinas, como tipo de máquina, método de provisionamento, conta de serviço, SO e versão do VDA, permitindo que você visualize e gerencie rapidamente seus recursos.
Propriedades do Modelo	Disponível apenas para catálogos provisionados por MCS.
	Exibe informações detalhadas de provisionamento para o catálogo selecionado, incluindo
	• Propriedades do Modelo de Máquina
	• Detalhes Específicos do Hypervisor
	• Propriedades do Perfil da Máquina
Máquinas	Exibe uma lista paginada de nomes de máquinas no catálogo selecionado.
Grupos de Entrega	Disponível para catálogos de PC Remoto.

GUIA	DESCRIÇÃO
	Exibe os grupos de entrega associados ao catálogo selecionado. Ele exibe o nome do grupo de entrega e a associação do catálogo.
Tags	Não disponível em ambientes multi-tenant.
	Exibe o nome da tag e a descrição das tags atribuídas ao catálogo de máquinas selecionado.
Gerenciamento do Ambiente de Trabalho	Visível apenas quando o serviço WEM é provisionado e acessível.
	Exibe as configurações de otimização do sistema de Gerenciamento do Ambiente de Trabalho.
Insights de Custo	Aplicável apenas a catálogos Azure MCS, isso exibe
	• Custo total incorrido nos últimos 30 dias.
	• Uma comparação entre o custo total atual de 30 dias e o período anterior de 30 dias.
	O acesso requer a permissão Citrix **Gerenciamento de Custos > Gerenciar > Ler custo** (padrão para Administradores de Nuvem) para visualizar a guia, e a permissão Azure `Microsoft.CostManagement/query/read` para visualizar os detalhes de custo.
Solução de problemas	Exibe erros ou avisos do catálogo com ações recomendadas.

Adicionar máquinas a um catálogo

Antes de começar:

- Certifique-se de que o host de virtualização (hipervisor ou provedor de serviços em nuvem) tenha processadores, memória e armazenamento suficientes para acomodar as máquinas adicionais.
- Certifique-se de ter contas de computador do Active Directory não utilizadas suficientes. Se você estiver usando contas existentes, o número de máquinas que você pode adicionar é limitado pelo número de contas disponíveis.
- Se você usar o Studio para criar contas de computador do Active Directory para as máquinas adicionais, você deve ter a permissão de administrador de domínio apropriada.

> **Dica:**

> Se a conta do Citrix DaaS usada para adicionar máquinas ao catálogo de máquinas tiver permissões de AD restritas, adicione todos os Cloud Connectors que você pretende usar na tela **Fazer logon em...**.

> Para adicionar máquinas a um catálogo:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo de máquinas e, em seguida, selecione **Adicionar máquinas** na barra de ações.
3. Na página **Máquinas Virtuais**, selecione o número de máquinas virtuais a serem adicionadas.
4. Na página **Identidades da Máquina**, configure as definições da seguinte forma:
    - Selecione uma identidade da lista.
    - Se aplicável, indique se deseja criar contas ou usar as existentes, e o local (domínio) para essas contas.

      Se houver contas do Active Directory existentes insuficientes para o número de VMs que você está adicionando, selecione o domínio e o local onde as contas são criadas.

      Se você usar contas do Active Directory existentes, navegue até as contas ou selecione **Importar** e especifique um arquivo `.csv` contendo nomes de contas. Certifique-se de que há contas suficientes para todas as máquinas que você está adicionando. O Studio gerencia essas contas. Permita que essa interface redefina as senhas de todas as contas, ou especifique a senha da conta, que deve ser a mesma para todas as contas.

- Se este pool de identidades for usado por outros catálogos, você não poderá alterá-lo para um pool diferente usando o Studio. Em vez disso, use o cmdlet PowerShell **Set-ProvScheme**. Para obter mais informações, consulte a Documentação do SDK do Citrix Virtual Apps and Desktops.
- Especifique um esquema de nomenclatura de conta, usando sinais de cerquilha para indicar onde números ou letras sequenciais aparecem. Por exemplo, um esquema de nomenclatura de PC-Sales-## (com 0-9 selecionado) resulta em contas de computador nomeadas PC-Sales-01, PC-Sales-02, PC-Sales-03 e assim por diante.
- Opcionalmente, você pode especificar com o que os nomes das contas começam.

  Ao especificar com o que os nomes das contas começam, esteja ciente do seguinte cenário: Se os números ou letras iniciais já estiverem em uso, a primeira conta criada será nomeada usando os números ou letras não utilizados mais próximos a partir daí.

  Consulte Gerenciar o número de sequência do nome da máquina para personalizar o número de sequência das máquinas, que são implantadas usando MCS, por meio de comandos PowerShell.

5. Na página **Credenciais de Domínio**, selecione **Inserir credenciais** e insira credenciais de usuário com permissões suficientes para criar contas de máquina.

As máquinas são criadas como um processo em segundo plano e podem levar muito tempo ao criar muitas máquinas. A criação da máquina continua mesmo se você fechar o Studio.

Usar arquivos CSV para adicionar máquinas em massa a um catálogo

Você pode adicionar máquinas em massa usando arquivos CSV. O recurso está disponível para todos os catálogos, exceto os catálogos provisionados via MCS.

Para adicionar máquinas em massa a um catálogo, conclua as seguintes etapas:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo de máquinas e, em seguida, selecione **Adicionar Máquinas** na barra de ações. A janela **Adicionar Máquinas** é exibida.
3. Selecione **Adicionar Arquivo CSV**. A janela **Adicionar Máquinas em Massa** é exibida.
4. Selecione **Baixar Modelo CSV**.
5. Preencha o arquivo de modelo.
6. Arraste ou navegue até o arquivo para carregá-lo.
7. Selecione **Validar** para realizar verificações de validação em sua importação.

8. Selecione **Importar** para concluir o processo.

Considerações ao usar arquivos CSV para adicionar máquinas

> **Nota:**
>
> - Para usuários que não são do Active Directory, você deve digitar seus nomes neste formato: `<identity provider>:<user name>`. Exemplo: `AzureAD:username`.
> - Os nomes das VMs diferenciam maiúsculas de minúsculas. Ao inserir caminhos de VM, certifique-se de inserir os nomes das VMs corretamente.

> Ao editar o arquivo de modelo CSV, tenha o seguinte em mente:

- O recurso oferece mais flexibilidade para adicionar máquinas em massa por meio de um arquivo CSV. No arquivo, você pode adicionar apenas máquinas (para uso com atribuições automáticas de usuário) ou adicionar máquinas juntamente com atribuições de usuário. Digite seus dados no seguinte formato:
  - Para pares de conta de máquina e nome de usuário (samName):
  - Domain\ComputerName1, Domain\Username1
  - Domain\ComputerName2, Domain\Username1;Domain\Username2
  - Domain\ComputerName3, AzureAD:username
  - Somente para contas de máquina:
  - Domain\ComputerName1
  - Domain\ComputerName2
  - Para pares de VM e nome de usuário:
  - XDHyp: \Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\ComputerName1,Domai
  - XDHyp: \Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\ComputerName2,Domai
  - Somente para VMs:
  - XDHyp: \Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\ComputerName1

  - XDHyp: \Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\ComputerName2

    Por exemplo: `XDHyp:\Connections\xpace-scale\East US.region\vm.folder\wsvdaV3-2.vm`

    onde,

  - `xpace-scale` é o ConnectionName: O nome da conexão que você inseriu em **Hospedagem > Adicionar Conexões e Recursos**. Para obter mais informações, consulte Criar uma conexão e recursos.
  - `East US.region` é o RegionName: O nome da região com `.region` como extensão.
  - `wsvdaV3-2.vm` é o VMName: O nome da máquina virtual com `.vm` como extensão.

- O número máximo de máquinas que um arquivo pode conter é 1.000. Para importar mais de 1.000 máquinas, distribua-as em arquivos diferentes e importe esses arquivos um por um. Recomendamos que você importe no máximo 1.000 máquinas. Caso contrário, a criação do catálogo pode levar muito tempo para ser concluída.

Você também pode exportar máquinas de um catálogo na mesma página **Adicionar Máquinas**. O CSV exportado de máquinas pode então ser usado como um modelo ao adicionar máquinas em massa. Para exportar máquinas:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo de máquinas e, em seguida, selecione **Adicionar Máquinas** na barra de ações. A janela **Adicionar Máquinas** é exibida.
3. Selecione **Exportar para arquivo CSV**. Um arquivo CSV contendo uma lista das máquinas é baixado.
4. Abra o arquivo CSV para adicionar ou editar máquinas conforme necessário. Para adicionar máquinas em massa usando o arquivo CSV salvo, consulte a seção anterior, Usar arquivos CSV para adicionar máquinas em massa a um catálogo.

> **Nota:**

> - Este recurso não está disponível para Acesso Remoto a PC e catálogos provisionados por MCS.

- A exportação e importação de máquinas em arquivos CSV é suportada apenas entre catálogos do mesmo tipo.

Registrar máquinas em catálogos usando a ferramenta de registro VDA WebSocket

A ferramenta de registro de VDA WebSocket facilita o registro baseado em token para máquinas VDA. Esta ferramenta ajuda você a converter uma conexão em uma conexão WebSocket adicionando o VDA ao catálogo de máquinas usando o token de registro.

Nota:

Esta ferramenta foi projetada para registrar máquinas VDA que não foram registradas em nenhum catálogo de máquinas.

Siga as instruções para executar a ferramenta de registro:

1. Faça login no VDA.
2. Localize a ferramenta `EnrollMachine.exe`, em `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool`.
3. Execute a ferramenta com os parâmetros de entrada apropriados. Por exemplo, `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

A tabela a seguir descreve os parâmetros de entrada da ferramenta de registro:

NOME DO PARÂMETRO	OBRIGATÓRIO	DESCRIÇÃO	EXEMPLO
`-websocket_token_stdin`	Sim	Lê o token de registro.	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		Lê o token de registro diretamente do parâmetro da linha de comando.	`.\EnrollMachine.exe -websocket_token_string:<token>`

NOME DO PARÂMETRO	OBRIGATÓRIO	DESCRIÇÃO	EXEMPLO
`-websocket_token_file:[token-file-path]`		Lê o token de registro do caminho fornecido.	`.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt`
`log:[log-file-path]`	Não	Mostra os logs da ferramenta de registro.	`.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]`
`-help`	Não	Mostra um breve texto de ajuda.	`.\EnrollMachine.exe -help`

Após o registro bem-sucedido, você receberá uma mensagem de sucesso na ferramenta e nos logs. Certifique-se de fazer login no Studio para verificar se a máquina VDA foi adicionada ao catálogo e se o status da máquina está registrado.

Solução de problemas

Por padrão, você pode encontrar os logs da ferramenta de registro em:

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

Se você especificou um caminho diferente para os logs, pode usar `log:[log-file-path]` para recuperar seus logs.

A tabela a seguir lista os códigos retornados pela ferramenta de registro:

CÓDIGO	STRING	DESCRIÇÃO
0	Sucesso	O VDA foi adicionado com sucesso ao catálogo de máquinas.

CÓDIGO	STRING	DESCRIÇÃO
-1	ArgumentoInválido	O parâmetro de entrada no token de registro é inválido.
-2	BrokerAgentNãoEncontrado	O serviço do agente do broker não foi encontrado.
-3	TokenInválido	O token inserido é inválido.
-4	ClaimsObrigatóriosDoTokenAusentes	As declarações (claims) obrigatórias para o token estão ausentes, por exemplo, CustomerId ou URIs de Registro.
-5	ErroInterno	Ocorreu um erro geral.
-6	TempoEsgotado	A tarefa expirou.
-7	FalhaAoDeterminarStatusADDaMáquina	O serviço que retorna o status de ingresso da máquina no AD falhou.
-8	MáquinaADFalhouAoEncontrarSid	O serviço que retorna o Sid da máquina AD falhou.
-9	FalhaNaSolicitaçãoDeInscrição	A solicitação falhou devido a um erro HTTP.
-10	RespostaDeInscriçãoComCamposObrigatóriosAusentes	A resposta da ferramenta de inscrição está faltando o parâmetro `VirtualSiteId`.
-11	PermissãoInsuficiente	Você não tem a permissão necessária para executar a tarefa.
-12	FalhaAoDeterminarStatusDeAdesãoAadDaMáquina	O serviço que verifica o status de adesão ao AD da máquina retorna um erro.

CÓDIGO	STRING	DESCRIÇÃO
-13	AadMáquinaFalhouAoEncontrarDeviceId	O parâmetro adicional `AAD device id` adicionado pelo sistema está vazio.
-14	AadDeviceIdNãoVálido	O parâmetro adicional `AAD device id` adicionado pelo sistema não é um GUID válido.
-15	NenhumEndereçoMacVálido	Endereço MAC inválido.
-16	FailedToGetComputerHostNameForVdaInstanceName	Falha ao obter o nome do host do computador para definir o parâmetro adicional `VdaInstanceName`.
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	Falha ao abrir a chave de registro do VDA para gravar a lista de Delivery Controllers.
-18	O token com falha atingiu a contagem máxima	O token com falha atingiu a contagem máxima.

Excluir máquinas de um catálogo

Depois de excluir uma máquina de um catálogo de máquinas, os usuários não poderão mais acessá-la, portanto, antes de excluir uma máquina, certifique-se de que:

- Os dados do usuário foram copiados ou não são mais necessários.
- Todos os usuários estão desconectados. Ativar o modo de manutenção impede que novas conexões sejam feitas a uma máquina.
- As máquinas estão desligadas.

Para excluir máquinas de um catálogo:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Exibir Máquinas** na barra de ações.
3. Selecione uma ou mais máquinas e, em seguida, selecione **Excluir** na barra de ações.

4. Se você estiver excluindo máquinas persistentes do catálogo, escolha se deseja excluí-las também do hipervisor ou do serviço de nuvem. Se você optar por excluí-las, indique se deseja reter, desabilitar ou excluir suas contas do Active Directory.

Ao excluir máquinas persistentes de um catálogo do Azure Resource Manager, as máquinas e os grupos de recursos associados são excluídos do Azure, mesmo que você opte por retê-los.

Ao excluir máquinas não persistentes de um catálogo, elas são automaticamente excluídas do hipervisor ou do serviço de nuvem.

Editar um catálogo

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Editar Catálogo de Máquinas** na barra de ações.
3. Na página **Escopos**, altere os escopos.
4. Na página **NIC**, execute as seguintes ações:

   - Para alterar o mapeamento de sub-rede de uma NIC, selecione uma rede no campo **Rede Associada**.
   - Para adicionar um mapeamento de sub-rede, selecione **Adicionar NIC**, selecione uma rede no campo **Rede Associada** e clique em **Salvar**.

   Somente as sub-redes presentes no host associado ao catálogo aparecem no campo **Rede Associada**.

   Você só pode adicionar NIC a catálogos de máquinas do Azure sem perfis de máquina.

> **Nota:**
>
> - Para catálogos de máquinas AWS, você não pode mapear a mesma sub-rede para mais de uma NIC.
> - Para catálogos de máquinas com perfis de máquina, o número de NICs no catálogo deve ser igual ao número de NICs no perfil de máquina.
> - Este recurso não é compatível com hipervisores IBM Cloud.
> - Este recurso é compatível apenas com o Nutanix Prism Element em hipervisores Nutanix.

5. Na página **Atualização do VDA**, altere ou selecione a versão do VDA para a qual deseja atualizar. Para obter mais informações, consulte Atualização do VDA.
6. Você pode ver páginas adicionais dependendo do tipo de catálogo.

   Para catálogos criados usando uma imagem do Azure Resource Manager, as seguintes páginas estão visíveis. Lembre-se de que as alterações feitas se aplicam apenas às máquinas que você adicionar ao catálogo posteriormente. As máquinas existentes permanecem inalteradas.

   - Na página **Máquinas Virtuais**, altere o tamanho da máquina e as zonas de disponibilidade onde você deseja criar máquinas.

     > **Nota:**
     >
     > - Somente os tamanhos de máquina compatíveis com o catálogo são exibidos.
     > - Se necessário, selecione **Mostrar apenas tamanhos de máquina usados em outros catálogos de máquinas** para filtrar a lista de tamanhos de máquina.
     > - Para catálogos do Azure, se **ZRS** for a redundância de armazenamento na página Tipos de Armazenamento e Licença, você receberá um aviso sugerindo que limpe a seleção de zona e deixe o Azure gerenciar as zonas de disponibilidade da VM.

   - Na página **Perfil da Máquina**, escolha se deseja usar ou alterar um perfil de máquina.

     > **Nota:**
     >
     > Para catálogos do Azure, ao modificar um perfil de máquina que inclui zonas de disponibilidade e escolher ZRS para redundância de armazenamento, um aviso sugere que você limpe a seleção de zona.

   - (Somente quando o catálogo é configurado com um host de grupo dedicado) Na página **Grupo de host dedicado**, escolha se deseja alterar um grupo de host.
   - Na página **Tipos de Armazenamento e Licença**, escolha se deseja alterar o tipo de redundância de armazenamento (para catálogo do Azure), tipo de armazenamento, tipo de

licença e configurações da Galeria de Computadores do Azure (disponível apenas quando **Colocar imagem preparada na Galeria do Azure** estiver em uso).

> **Nota:**
>
> Se a configuração recém-selecionada não suportar o tamanho atual da máquina, uma caixa de diálogo de aviso aparecerá, informando que a alteração da configuração redefine a configuração de tamanho da máquina. Se você optar por continuar, um ponto vermelho aparecerá ao lado do menu **Máquinas Virtuais**, solicitando que você selecione um novo tamanho de máquina.

Para obter mais informações sobre as configurações disponíveis nas páginas, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Para catálogos de Acesso Remoto a PC, as seguintes páginas estão visíveis:

- Na página **Gerenciamento de Energia**, altere as configurações de gerenciamento de energia e selecione uma conexão de gerenciamento de energia.
- Na página **Unidades Organizacionais**, adicione ou remova UOs do Active Directory.

7. Na página **Descrição**, altere a descrição do catálogo.
8. Clique em **Aplicar** para aplicar as alterações feitas e clique em **Salvar** para sair.

Renomear um catálogo

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Renomear Catálogo de Máquinas** na barra de ações.
3. Insira o novo nome.

Excluir um catálogo

Antes de excluir um catálogo, certifique-se de que:

- Todos os usuários estão desconectados e nenhuma sessão desconectada está em execução.
- O modo de manutenção está ativado para todas as máquinas no catálogo para que novas conexões não possam ser feitas.
- Todas as máquinas no catálogo estão desligadas.

- O catálogo não está associado a um grupo de entrega. Em outras palavras, o grupo de entrega não contém máquinas do catálogo.

Para excluir um catálogo:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo, selecione **Mais** na barra de ações e, em seguida, selecione **Excluir Catálogo de Máquinas**.
3. Se o catálogo contiver máquinas persistentes, indique se deseja excluir essas máquinas do hipervisor ou do serviço de nuvem também. Se você optar por fazer isso, escolha se deseja reter, desabilitar ou excluir suas contas de computador do Active Directory.
4. Se necessário, selecione **Ocultar progresso** para executar a exclusão em segundo plano.

> **Nota:**
>
> - Ao excluir um catálogo do Azure Resource Manager, as máquinas e os grupos de recursos associados são excluídos do Azure, mesmo que você opte por retê-los.
> - Ao excluir um catálogo que contém máquinas não persistentes, essas máquinas são excluídas do hipervisor ou do serviço de nuvem.
> - Quando o hipervisor ou o serviço de nuvem está inacessível durante a exclusão do catálogo, a exclusão do catálogo e da VM falha. Se necessário, você pode optar por excluir os registros da VM apenas do seu banco de dados do site Citrix. Para fazer isso, selecione o catálogo de máquinas no nó **Catálogos de Máquinas** e, em seguida, execute a exclusão mostrada na guia **Solução de problemas**. Lembre-se de que esta ação deixa as VMs intactas no host.

Gerenciar contas de computador do Active Directory em um catálogo

Para gerenciar contas do Active Directory em um catálogo de máquinas, você pode:

- Liberar contas de máquina não utilizadas removendo contas de computador do Active Directory de catálogos de sessão única e multi-sessão. Essas contas podem então ser usadas para outras máquinas.
- Adicionar contas para que, quando mais máquinas forem adicionadas ao catálogo, as contas de computador já estejam no lugar. Não use uma barra (/) em um nome de OU.

Para gerenciar contas do Active Directory:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Gerenciar contas AD** na barra de ações.
3. Escolha se deseja adicionar ou excluir contas de computador. Se você adicionar contas, especifique o que fazer com as senhas das contas: redefina todas elas ou insira uma senha que se aplique a todas as contas.

   Você pode redefinir senhas se não souber as senhas atuais das contas; você deve ter permissão para realizar uma redefinição de senha. Se você inserir uma senha, a senha será alterada nas contas à medida que forem importadas. Se você excluir uma conta, escolha se a conta em um Active Directory deve ser mantida, desabilitada ou excluída.

Você também pode indicar se as contas do Active Directory devem ser retidas, desabilitadas ou excluídas ao remover máquinas de um catálogo ou excluir um catálogo.

Alterar a imagem mestre de um catálogo

Recomendamos que você salve cópias ou instantâneos de imagens antes de alterar a imagem mestre de um catálogo. O banco de dados mantém um registro histórico das imagens usadas com cada catálogo de máquinas. Se os usuários encontrarem problemas com a nova imagem que você implantou em seus desktops, você poderá reverter para a versão anterior, minimizando o tempo de inatividade do usuário. Não exclua, mova ou renomeie imagens. Caso contrário, você não poderá reverter a imagem mestre.

> **Importante:**

> Ao alterar a imagem mestre para um catálogo persistente, considere o seguinte: apenas as máquinas que você adicionar ao catálogo posteriormente serão criadas usando a nova imagem. Não implementamos a nova imagem para máquinas existentes no catálogo.

> Depois que uma máquina é atualizada, ela reinicia automaticamente.

Converter catálogos provisionados por MCS de imagens mestre para imagens preparadas

Para converter um catálogo provisionado por MCS de uma imagem mestre para uma imagem preparada, siga estas etapas:

1. Clique em **Catálogos de Máquinas** no painel esquerdo e selecione um catálogo de máquinas que você deseja converter. Clique com o botão direito e selecione **Converter para Imagem Preparada**.
2. Na página **Imagem**, selecione uma imagem preparada.
3. Na página **Estratégia de implantação**, selecione quando você deseja atualizar este catálogo com a imagem preparada selecionada.
4. Na página **Resumo**, verifique os detalhes e clique em **Concluir**.
5. Verifique os detalhes do catálogo de máquinas convertido em **Propriedades do Modelo**.

Atualmente, este recurso está disponível apenas para ambientes de virtualização Azure e VMware.

Atualizar ou criar uma imagem

Antes de alterar a imagem mestre de um catálogo, prepare uma nova imagem em seu hipervisor host, atualizando uma imagem existente ou criando uma.

1. No seu hipervisor ou provedor de serviços em nuvem, tire um instantâneo da VM atual e dê um nome significativo ao instantâneo. Este instantâneo pode ser usado para reverter a imagem mestre.
2. Se necessário, ligue a imagem e faça logon.
3. Instale atualizações ou faça as alterações necessárias na imagem.
4. Se a imagem usar um Personal vDisk, atualize o inventário.
5. Desligue a VM.
6. Tire um instantâneo da VM e dê um nome significativo ao instantâneo que seja reconhecido ao alterar a imagem mestre.

> **Nota:**
>
> Embora você possa criar um instantâneo usando a interface de gerenciamento, recomendamos que você crie um instantâneo usando o console de gerenciamento do hipervisor e, em seguida, selecione esse instantâneo no Studio. Isso permite que você forneça um nome e uma descrição significativos, em vez de um nome gerado automaticamente. Para imagens de GPU, você pode alterar a imagem apenas através do console XenServer XenCenter®.

Alterar a imagem mestre

Para implantar uma nova imagem mestre em todas as máquinas de um catálogo:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Alterar Imagem Mestre** na barra de ações.
3. Na página **Imagem**, selecione o host e a imagem que você deseja implantar.

   > **Dica:**
   >
   > Para um catálogo criado por MCS, você pode anotar sua imagem adicionando uma nota para a imagem. Uma nota pode conter até 500 caracteres. Cada vez que você altera a imagem mestre, uma entrada relacionada à nota é criada, independentemente de você adicionar uma nota. Se você atualizar um catálogo sem adicionar uma nota, a entrada aparecerá como nula (-). Para visualizar o histórico de notas da imagem, selecione o catálogo, clique em **Propriedades do Modelo** no painel inferior e, em seguida, clique em **Exibir histórico de notas**.

4. Na página **Estratégia de Implantação**, escolha quando as máquinas no catálogo de máquinas serão alteradas com a nova imagem: no próximo desligamento ou imediatamente.

   > **Nota:**
   >
   > A página **Estratégia de Implantação** não está disponível para VMs persistentes porque a implantação é aplicável apenas a VMs não persistentes.

5. Verifique as informações na página **Resumo** e, em seguida, selecione **Concluir**. Cada máquina é reiniciada automaticamente após ser atualizada.

   Para acompanhar o progresso da atualização, localize o catálogo em **Catálogos de Máquinas** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo. Para um catálogo não persistente, você pode acompanhar os status de atualização da imagem através da coluna **Atualização da Imagem**, incluindo **Totalmente atualizado**, **Parcialmente atualizado**, **Atualização pendente** e **Preparando imagem**.

   > **Dica:**

> Para exibir a coluna **Atualização da Imagem**, selecione o ícone **Colunas a Exibir** na barra de ações, selecione **Catálogo de Máquinas > Status da Imagem** e, em seguida, clique em **Salvar**.

Se você estiver atualizando um catálogo usando o SDK do PowerShell, poderá especificar um modelo de hipervisor (`VMTemplates`), como uma alternativa a uma imagem ou um instantâneo de uma imagem.

Para implantar uma nova imagem mestre no catálogo de máquinas baseado no Azure:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo do Azure e, em seguida, selecione **Alterar Imagem Mestre** na barra de ações.
3. Na página **Alterar Imagem Mestre**, selecione uma imagem em Imagem mestre. A lâmina lista todas as imagens que pertencem à mesma região que as dos Recursos.

Estratégia de implantação

A alteração da imagem no próximo desligamento afetará imediatamente todas as máquinas que não estão em uso no momento, ou seja, máquinas que não têm uma sessão de usuário ativa. Um sistema em uso recebe a atualização quando a sessão ativa atual termina.

> **Nota:**
>
> A estratégia de implantação é aplicável apenas a VMs não persistentes.
>
> Considere o seguinte:
>
> - Novas sessões não podem ser iniciadas até que a atualização seja concluída nas máquinas aplicáveis.
> - Para máquinas de sessão única, as máquinas são atualizadas imediatamente quando a máquina não está em uso ou quando os usuários não estão logados.
> - Para um SO multi-sessão com máquinas filhas, as reinicializações não ocorrem automaticamente. Para aplicar a imagem mestre atualizada, reinicie as máquinas usando Studio, PowerShell ou Workspace. A reinicialização das máquinas ou dos hipervisores não aplica a atualização.

> **Dica:**
>
> Limite o número de máquinas sendo reiniciadas usando as configurações avançadas para uma conexão de host. Use essas configurações para modificar as ações tomadas para um determinado catálogo; as configurações avançadas variam dependendo do hipervisor.

Reverter a imagem mestre

Depois de implantar uma imagem atualizada ou nova, você pode revertê-la. Isso pode ser necessário se ocorrerem problemas com as máquinas recém-atualizadas. Ao reverter, as máquinas no catálogo são revertidas para a última imagem funcional. Quaisquer novos recursos que exijam a imagem mais recente não estarão mais disponíveis. Assim como na implantação, reverter uma máquina inclui uma reinicialização.

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione o catálogo e, em seguida, selecione **Reverter Imagem Mestra** na barra de ações.
3. Especifique quando aplicar a imagem anterior às máquinas, conforme descrito para a operação de implantação.

A reversão é aplicada apenas às máquinas que precisam ser revertidas. Para máquinas que não foram alteradas para a imagem nova ou atualizada (por exemplo, máquinas com usuários que não fizeram logoff), os usuários não recebem mensagens de notificação e não são forçados a fazer logoff.

Para acompanhar o progresso da reversão, localize o catálogo em **Catálogos de Máquinas** para visualizar a barra de progresso em linha e o gráfico de progresso passo a passo.

Você não pode reverter em certos cenários, incluindo os seguintes. (A opção **Reverter Imagem Mestra** não está visível).

- Você não tem permissão para reverter.
- O catálogo não foi criado usando o MCS.
- O catálogo foi criado usando uma imagem do disco do SO.
- O snapshot usado para criar o catálogo foi corrompido.
- As alterações do usuário nas máquinas do catálogo não persistem.
- As máquinas no catálogo estão em execução.

Alterar o nível funcional ou desfazer a alteração

Altere o nível funcional para o catálogo de máquinas depois de atualizar os VDAs nas máquinas para uma versão mais recente. Recomendamos atualizar todos os VDAs para a versão mais recente para permitir o acesso a todos os recursos mais novos.

Antes de alterar o nível funcional para um catálogo de máquinas:

- Inicie as máquinas atualizadas para que elas se registrem no Citrix DaaS. Isso permite que a interface de gerenciamento determine que as máquinas no catálogo precisam de atualização.

Para alterar o nível funcional de um catálogo:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione o catálogo. A guia **Detalhes** no painel inferior exibe as informações da versão.
3. Selecione **Alterar Nível Funcional**. Se a interface de gerenciamento detectar que o catálogo deve alterar o nível funcional, ela exibirá uma mensagem. Siga as instruções. Se uma ou mais máquinas não puderem ser alteradas, uma mensagem explicará o motivo. Para garantir que todas as máquinas funcionem corretamente. Recomendamos que você resolva esses problemas antes de clicar em **Alterar**.

Após a conclusão da atualização do catálogo, você pode reverter as máquinas para suas versões VDA anteriores selecionando o catálogo e, em seguida, selecionando **Desfazer Alteração de Nível Funcional** na barra de ações.

Clonar um catálogo

Antes de clonar um catálogo, esteja ciente das seguintes considerações:

- Você não pode alterar as configurações associadas ao sistema operacional e ao gerenciamento de máquinas. O catálogo clonado herda essas configurações do original.

  > **Nota:**
  >
  > Se você selecionar um catálogo do Azure para clonar e selecionar uma imagem Mestra, o painel listará todas as imagens que pertencem à mesma região que as dos Recursos.

- A clonagem de um catálogo pode levar algum tempo para ser concluída. Se necessário, selecione **Ocultar progresso** para executar a clonagem em segundo plano.

- O catálogo clonado herda o nome do original e tem o sufixo `Copy`. Você pode alterar o nome. Consulte Renomear um catálogo.
- Após a conclusão da clonagem, certifique-se de atribuir o catálogo clonado a um grupo de entrega.
- Você pode criar um catálogo vazio por clonagem. Durante a clonagem do catálogo, você pode definir o número de máquinas como zero para catálogos provisionados por MCS e não adicionar máquinas para catálogos não provisionados por MCS.

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione um catálogo e, em seguida, selecione **Clonar** na barra de ações.
3. Na janela **Clonar Catálogo de Máquinas Selecionado**, visualize as configurações do catálogo clonado e configure as configurações conforme aplicável. Selecione **Avançar** para prosseguir para a próxima página.
4. Na página **Resumo**, visualize um resumo das configurações e selecione **Concluir** para iniciar a clonagem.
5. Se necessário, selecione **Ocultar progresso** para executar a clonagem em segundo plano.

Organizar catálogos usando pastas

Você pode criar pastas para organizar catálogos para facilitar o acesso. Por exemplo, você pode organizar catálogos por tipo de imagem ou por estrutura organizacional.

> **Dica:**
>
> Você pode definir sua exibição padrão preferida (exibição de pasta ou lista) para o nó Catálogos de Máquinas clicando no ícone **Pasta** no canto superior direito da barra de ações.

Funções necessárias

Por padrão, você precisa ter a seguinte função interna para criar e gerenciar pastas de catálogo: Administrador de Nuvem, Administrador Completo ou Administrador de Catálogo de Máquinas. Se necessário, você pode personalizar funções para criar e gerenciar pastas de catálogo. Para obter mais informações, consulte Permissões necessárias.

Criar uma pasta de catálogo

Antes de começar, planeje como organizar seus catálogos. Considere o seguinte:

- Você pode aninhar pastas em até cinco níveis de profundidade (excluindo a pasta raiz padrão).
- Uma pasta de catálogo pode conter catálogos e subpastas.
- Todos os nós no Studio (como **Catálogos de Máquinas**, **Grupos de Entrega**, **Aplicativos** e **Grupos de Aplicativos**) compartilham a mesma árvore de pastas no back-end. Para evitar conflitos de nomes ao renomear ou mover pastas, use nomes exclusivos para pastas de primeiro nível em diferentes nós.

  Se você criar uma pasta usando o cmdlet SDK `New-BrokerAdminFolder` e quiser que ela apareça no nó **Catálogos de Máquinas**, você deve adicionar os metadados `ContainsMachineCatalogs` usando o cmdlet `Set-BrokerAdminFolderMetadata`.

  Exemplo:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsMachineCatalogs -Value true
  ```

Para criar uma pasta de catálogo, siga estas etapas:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Criar Pasta** na barra de **Ações**.
3. Digite um nome para a nova pasta e clique em **Concluído**.

Dica:

Se você criar uma pasta em um local não intencional, poderá arrastá-la para o local correto.

Mover um catálogo

Você pode mover um catálogo entre pastas. As etapas detalhadas são as seguintes:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Visualize catálogos por pasta. Você também pode ativar **Visualizar tudo** acima da hierarquia de pastas para visualizar todos os catálogos de uma vez.
3. Clique com o botão direito em um catálogo e selecione **Mover Catálogo de Máquinas**.
4. Selecione a pasta para a qual você deseja mover o catálogo e clique em **Concluído**.

> **Dica:**
>
> Você pode arrastar um catálogo para uma pasta.

Gerenciar pastas de catálogo

Você pode excluir, renomear e mover pastas de catálogo.

Você pode excluir uma pasta somente se ela e suas subpastas não contiverem catálogos.

Para gerenciar uma pasta, siga estas etapas:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione uma ação na barra **Ação** conforme necessário:
   - Para renomear a pasta, selecione **Renomear Pasta**.
   - Para excluir a pasta, selecione **Excluir Pasta**.
   - Para mover a pasta, selecione **Mover Pasta**.
3. Siga as instruções na tela para concluir as etapas restantes.

Permissões necessárias

A tabela a seguir lista as permissões necessárias para realizar ações em pastas de catálogo.

AÇÃO	PERMISSÕES NECESSÁRIAS
Criar pastas de catálogo	Criar Pasta de Catálogo de Máquina
Excluir pastas de catálogo	Remover Pasta de Catálogo de Máquina
Mover pastas de catálogo	Mover Pasta de Catálogo de Máquina
Renomear pastas de catálogo	Editar Pasta de Catálogo de Máquina
Mover catálogos para pastas	Editar Pasta de Catálogo de Máquina e Editar Propriedades do Catálogo de Máquina

Atualizar VDAs

Você pode usar a interface do Studio para atualizar VDAs com facilidade. Para obter mais informações e orientações passo a passo, consulte a documentação de Citrix VDA Upgrade Service.

Gerenciar configurações de otimização de experiência para um catálogo

Antes de começar, certifique-se de que sua implantação do serviço **Workspace Environment Management (WEM)** esteja configurada. Para obter mais informações, consulte Introdução ao serviço Workspace Environment Management.

Permissões necessárias

Por padrão, a criação e o gerenciamento de conjuntos de configuração para catálogos de máquinas exigem a função de **Administrador Completo do WEM**, juntamente com uma das seguintes funções:

- **Administrador de Acesso Total**
- **Administrador de Nuvem**
- **Administrador de Catálogo de Máquinas**

Para permitir que outras funções gerenciem conjuntos de configuração, atribua a elas a permissão **Gerenciar conjuntos de configuração** e a função **Administrador Completo do WEM**.

Editar as configurações de otimização de experiência

Selecione uma opção de **Otimização de Experiência** para aplicar ao catálogo:

- **Aplicar configurações padrão:** Selecione esta opção para aplicar as configurações de otimização padrão, incluindo proteção automática contra picos de CPU e otimização inteligente de CPU.
- **Aplicar configurações personalizadas:** Insira um nome para criar um conjunto de configuração e, em seguida, personalize as configurações de otimização de acordo com seus requisitos. Alternativamente, você pode selecionar um conjunto de configuração existente.

Tentar novamente a criação do catálogo

> **Nota:**
>
> Este recurso se aplica apenas a catálogos MCS.

> Os catálogos com falha são marcados com um ícone de erro. Para ver os detalhes, vá para a guia **Solucionar problemas** de cada catálogo. Antes de tentar novamente a criação do catálogo, esteja ciente das seguintes considerações:

- Verifique primeiro as informações de solução de problemas e resolva os problemas. As informações descrevem os problemas encontrados e fornecem recomendações para resolvê-los.
- Você não pode alterar as configurações associadas a Sistema operacional e gerenciamento de máquina. O catálogo herda essas configurações do original.
- A criação pode levar algum tempo para ser concluída. Se necessário, selecione **Ocultar progresso** para executar a criação em segundo plano.

Para tentar novamente a criação de um catálogo, faça o seguinte:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione o catálogo e vá para a guia **Solucionar problemas**.
3. Clique no hiperlink de repetição para tentar novamente a criação do catálogo.
4. No assistente que aparece, altere as configurações onde for necessário. Se não houver necessidade de fazer alterações, você pode ir diretamente para a página **Resumo**.
5. Depois de terminar, selecione **Concluir** para iniciar a criação.

(Somente VDAs não provisionados pelo Citrix) Gerar e gerenciar tokens de registro

> **Nota:**
>
> Para executar esta tarefa, você deve ter a função de Administrador de Nuvem.

> Depois de decidir adotar o registro baseado em token para máquinas não provisionadas pelo Citrix, gere tokens por catálogo de máquina e, em seguida, compartilhe-os com os administradores de instalação do VDA.

Um token de registro apresenta:

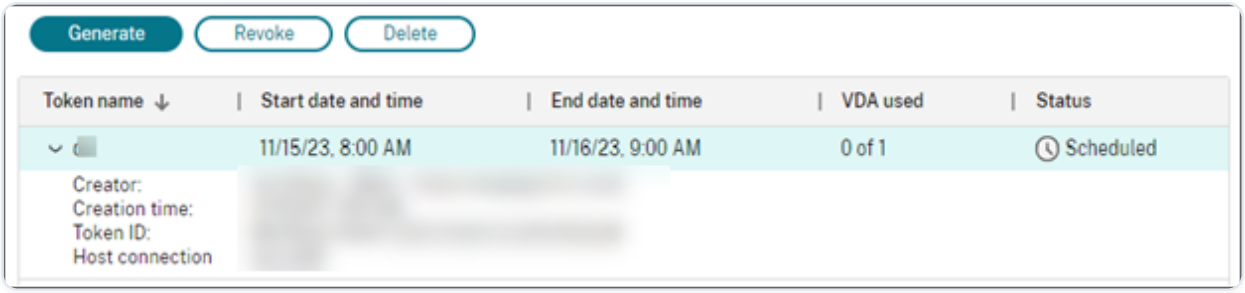
- Intervalo de registro: 1 a 5000 máquinas VDA

- Período de validade: até 14 dias

Para gerar um token para um catálogo usando o Studio, siga estas etapas:

1. Em **Catálogos de Máquinas**, localize um catálogo não provisionado por MCS, que tenha **Método de provisionamento: Manual** exibido na coluna **Contagem de Máquinas**.
2. Clique com o botão direito do mouse no catálogo e selecione **Gerenciar Tokens de Registro**.
3. Na página **Gerar token de registro** que aparece, forneça as seguintes informações do token:
   - Digite um nome para o token.
   - Insira seu período de validade. O período não deve ser superior a 14 dias. O token é válido apenas para o período especificado.
   - (Opcional) Selecione uma conexão de host para o gerenciamento de energia de VDAs registrados com o token. As opções incluem todas as conexões de host na zona deste catálogo.
   - Insira os limites de uso do token (entre 1 e 5000).
4. Clique em **Gerar**.
5. Na janela **Token gerado com sucesso** que aparece, copie o token e salve-o em um local seguro, ou clique em **Baixar** para fazer o download para a pasta **Downloads**.

   Um registro de token aparece na lista de tokens.



6. Compartilhe o token com os administradores de instalação do VDA.

   Para obter mais informações sobre como instalar o VDA e um token nas máquinas, consulte Instalar VDAs.

Gerenciar tokens

Você tem duas opções para revogar um token e torná-lo indisponível para o registro do VDA:

- Revogar: Revoga o token, mas o mantém na lista para fins de registro.
- Excluir: Revoga o token e o exclui da lista.

> **Nota:**
>
> Tokens expirados são excluídos automaticamente em 14 dias.

Usar PowerShell

Esta seção detalha como você pode gerenciar catálogos usando o PowerShell:

- Usar PowerShell para verificar o status de atualização do VDA e a versão do VDA
- Gerenciar o número de sequência do nome da máquina
- Adicionar descrições a uma imagem
- Redefinir disco do SO
- Reparar as informações de identidade de contas de computador ativas
- Alterar a configuração de rede para um catálogo de máquinas existente
- Gerenciar versões de um catálogo de máquinas
- Alterar a configuração de cache de um catálogo de máquinas existente
- Converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina
- Recuperar avisos e erros associados a um catálogo
- Excluir máquinas sem acesso ao hipervisor
- Atualizar propriedades de VMs individuais

Gerenciar o número de sequência do nome da máquina

Para personalizar o número de sequência das máquinas, que são implantadas usando MCS, por meio de comandos PowerShell, faça o seguinte:

1. Abra o PowerShell como administrador no Delivery Controller.
2. Execute o comando `asnp citrix*` para carregar os módulos Citrix.
3. Execute o seguinte comando para verificar a contagem inicial para o pool de identidade do catálogo:

   ```
   Get-AcctIdentityPool -IdentityPoolName xxx
   ```

   O `IdentityPoolName` é o nome do catálogo.

4. Se você quiser definir essa contagem para um valor diferente, execute o seguinte comando e especifique o StartCount como X:

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount X
   ```

5. Adicione as máquinas ao catálogo para que as máquinas sejam criadas com a contagem necessária.
6. Após criar as máquinas, execute o seguinte comando para redefini-lo para o valor original Y:

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount Y
   ```

Adicionar descrições a uma imagem

Você pode adicionar descrições informativas sobre alterações relacionadas a atualizações de imagem para catálogos de máquinas. Use esse recurso para adicionar uma descrição ao criar um catálogo ou ao atualizar uma imagem mestre existente para um catálogo. Você também pode exibir informações para cada imagem mestre no catálogo. Essa funcionalidade é útil para administradores que desejam adicionar rótulos descritivos ao atualizar uma imagem mestre usada por um catálogo, por exemplo, *Office 365 instalado*. Use os seguintes comandos para adicionar ou visualizar descrições de imagem:

- `NewProvScheme`. Um novo parâmetro, `masterImageNote` permite adicionar uma nota a uma imagem. Por exemplo:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName XenHu
-IdentityPoolName idPool1 -MasterImageVM XDHyp:
\HostingUnits\XenHU\Base.vm\Base.snapshot -MasterImageNote "Office365
installed"
```

- `Publish-ProvMasterVMImage`. Use este parâmetro para publicar a nota. Por exemplo:

`C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName MyScheme -MasterImageVM XDHyp:\HostingUnits\HostUnit1\RhoneCC_baseXP.vm\base.snapshot -MasterImageNote "Visual Studio 2019 installed"`

- `Get-ProvSchemeMasterVMImageHistory`. Exiba informações para cada imagem. Por exemplo:

`C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName MyScheme -Showall

VMImageHistoryUid : 3cba3a75-89cd-4868-989b-27feb378fec5

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

ProvisioningSchemeName : MyScheme

MasterImageVM : /Base.vm/base.snapshot

Data : 17/05/2021 09:27:50

MasterImageNote : Office365 instalado`

Redefinir disco do SO

Use o comando PowerShell `Reset-ProvVMDisk` para redefinir o disco do SO de uma VM persistente em um catálogo de máquinas criado pelo MCS. Atualmente, este recurso é aplicável a ambientes de virtualização AWS, Azure, Google Cloud, SCVMM, VMware e XenServer®.

Para executar o comando PowerShell com sucesso, certifique-se de que:

- As VMs de destino estão em um catálogo MCS persistente.
- O catálogo de máquinas MCS está funcionando corretamente. Isso implica que o esquema de provisionamento e o host existem, e o esquema de provisionamento tem entradas corretas.
- O hipervisor não está em modo de manutenção.
- As VMs de destino estão desligadas e em modo de manutenção.

Execute as seguintes etapas para redefinir o disco do SO:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute o comando PowerShell `Reset-ProvVMDisk` de uma das seguintes maneiras:
    - Especifique a lista de VMs como uma lista separada por vírgulas, e execute a redefinição em cada VM:

      ```
      Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
      -OS
      ```

    - Especifique a lista de VMs como uma saída do comando `Get-ProvVM`, e execute a redefinição em cada VM:

```
(Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
-OS
```

- Especifique uma única VM pelo nome:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

- Crie tarefas de redefinição separadas para cada uma das VMs retornadas pelo comando `Get-ProvVM`. Isso é menos eficiente porque cada tarefa executará as mesmas verificações redundantes, como verificação de capacidade do hipervisor, verificação de conexão para cada VM.

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
-ProvisioningSchemeName "xxx" -OS
```

4. Um prompt de confirmação aparece listando as VMs a serem redefinidas, juntamente com uma mensagem de aviso de que é uma operação irrecuperável. Se você não fornecer uma resposta e pressionar **Enter**, nenhuma outra ação será executada.

   Você pode executar o comando PowerShell `-WhatIf` para imprimir a ação que ele executaria e sair sem realizar a ação.

   Você também pode ignorar o prompt de confirmação usando um dos seguintes métodos:

   - Forneça o parâmetro `-Force`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Force
```

   - Forneça o parâmetro `-Confirm:$false`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Confirm:$false
```

   - Antes de executar o `Reset-ProvVMDisk`, altere `$ConfirmPreference` para 'None':

```
PS C:\Windows\system32> $ConfirmPreference='None'

PS C:\Windows\system32> $ConfirmPreference

None

PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
"xxx" -VMName "abc" -OS
```

Nota:

Não retire as VMs do modo de manutenção nem as ligue até a conclusão do processo de redefinição.

5. Execute `Get-ProvTask` para obter o status das tarefas retornadas pelo comando `Reset-ProvVMDisk`.

Reparar as informações de identidade de contas de computador ativas

Você pode redefinir as informações de identidade de contas de computador ativas que apresentam problemas relacionados à identidade. Você pode optar por redefinir apenas a senha da máquina e as chaves de confiança, ou redefinir toda a configuração do disco de identidade. Esta implementação é aplicável a catálogos de máquinas MCS persistentes e não persistentes.

Nota:

Atualmente, o recurso é suportado apenas para ambientes de virtualização AWS, Azure, GCP, SCVMM, VMware e XenServer.

Condições

Certifique-se do seguinte para redefinir o disco de identidade com êxito:

- Desligue e defina a VM para o modo de manutenção
- Não inclua o parâmetro -OS no comando PowerShell

Redefinir informações de identidade

Para redefinir as informações de identidade:

1. Abra a janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Redefina as informações de identidade.

   - Para redefinir apenas a senha da máquina e as chaves de confiança, execute o seguinte comando:

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     A descrição dos parâmetros usados no comando é a seguinte:

     - `IdentityAccountName`: O nome da conta de identidade que deve ser reparada.
     - `PrivilegedUserName`: Conta de usuário que tem permissão de gravação no provedor de identidade (AD ou Microsoft Entra ID).
     - `PrivilegedUserPassword`: Senha para PrivilegedUserName.
     - `Target`: Destino para a ação de reparo. Pode ser IdentityInfo para reparar a senha da conta/chave de confiança e UserCertificate para reparar os atributos de certificado de usuário de identidades de máquina híbridas do Microsoft Entra.

   - Para redefinir toda a configuração do disco de identidade, execute os seguintes comandos na seguinte ordem:

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     ```
     Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
     Identity
     ```

   - Para recriar completamente o disco de identidade:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
-Identity -Recreate
```

Nota:

Se a máquina estiver em uma versão VDA 2511 (Atualização 1) ou posterior e tiver a chave de registro definida para habilitar `MachineGuid` exclusivo (`HKLM:\Software\Citrix\MachineIdentityServiceAgent\EnableUniqueMachineGuid`), ela continuará usando o mesmo `MachineGuid` de antes, independentemente da configuração `-Recreate`

4. Digite **y** para confirmar a ação. Você também pode pular o prompt de confirmação usando o parâmetro `-Force`. Por exemplo:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. Execute `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` para verificar a configuração atualizada do disco de identidade. Os atributos do disco de identidade (por exemplo, `IdentityDiskId`) devem ser atualizados. O `StorageId` e o `IdentityDiskIndex` não devem ser alterados.

Alterar a configuração de rede para um catálogo de máquinas existente

Você pode alterar a configuração de rede para um catálogo de máquinas existente para que as novas VMs sejam criadas na nova sub-rede. Use o parâmetro `-NetworkMapping` no comando `Set-ProvScheme` para alterar a configuração de rede.

Para alterar a configuração de rede para um esquema de provisionamento existente, faça o seguinte:

1. Na janela do PowerShell, execute o comando `asnp citrix*` para carregar os módulos do PowerShell.
2. Execute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para acessar o caminho de rede que você deseja alterar.
3. Atribua uma variável à nova configuração de rede. Por exemplo:

```
$NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network
0.network"}
```

4. Execute `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap`.
5. Execute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para verificar a nova configuração de rede para o esquema de provisionamento existente.

Gerenciar versões de um catálogo de máquinas

Quando um catálogo de máquinas MCS é atualizado com o comando `Set-ProvScheme`, a configuração atual é salva como uma versão. Você pode então gerenciar as várias versões do catálogo de máquinas usando comandos PowerShell. Você pode:

- Ver a lista de versões de um catálogo de máquinas.
- Usar qualquer versão anterior para atualizar o catálogo de máquinas.
- Excluir manualmente uma versão se ela não for usada por uma VM desse catálogo de máquinas.
- Alterar o número máximo de versões a serem retidas pelo catálogo de máquinas (o padrão é 99).

Uma versão inclui as seguintes informações de um catálogo de máquinas:

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

Execute os seguintes comandos (fornecidos como exemplos) para gerenciar as várias versões de um catálogo de máquinas.

- Para ver os detalhes de configuração das várias versões de um catálogo de máquinas:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- Para ver os detalhes de configuração de uma versão específica de um catálogo de máquinas:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- Para ver o número total de versões associadas a um catálogo de máquinas:

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- Para usar qualquer versão anterior para atualizar o catálogo de máquinas:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- Para excluir manualmente uma versão se ela não for usada por uma VM desse catálogo de máquinas:

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- Para definir o número máximo de versões a serem retidas pelo catálogo de máquinas (o padrão é 99). Essa configuração é aplicada a todos os catálogos. Por exemplo, neste caso, um máximo de 15 versões será retido para todos os catálogos provisionados pelo MCS.

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

Se o número de versões atingir o número máximo de versões, uma nova versão não poderá ser criada se versões mais antigas estiverem em uso por qualquer uma das VMs no catálogo de máquinas. Nesse caso, faça uma das seguintes ações:

- Aumente o limite do número máximo de versões a serem retidas pelo catálogo de máquinas.
- Atualize algumas VMs que estão em versões mais antigas para que essas versões mais antigas não sejam mais referenciadas por nenhuma VM e possam ser excluídas.

Alterar a configuração de cache de um catálogo de máquinas existente

Depois de criar um catálogo não persistente com o MCSIO ativado, você pode usar o comando `Set-ProvScheme` para modificar os seguintes parâmetros:

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

Este recurso é atualmente aplicável a:

- Ambientes GCP e Microsoft Azure, e
- um catálogo não persistente com MCSIO ativado

Requisitos

Os requisitos para modificar a configuração do cache são:

- Atualize para a versão mais recente do VDA (2308 ou posterior).
- Habilite o parâmetro `UseWriteBackCache` para o catálogo de máquinas existente. Use `New-ProvScheme` para criar um catálogo de máquinas com `UseWriteBackCache` habilitado. Por exemplo:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `

-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

Alterar a configuração do cache

Execute o comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

Nota:

- O valor de `WriteBackCacheDiskSize` deve ser maior que zero, pois é necessário pelo menos 1 GB de armazenamento em disco de cache.
- O valor de `WriteBackCacheMemorySize` deve ser menor que o tamanho da memória do catálogo de máquinas.
- Essas alterações afetam apenas as novas VMs adicionadas ao catálogo após a alteração. As VMs existentes não são afetadas por essas alterações.

Converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina

Você pode usar uma VM, especificação de modelo (no caso do Azure), ou modelo de inicialização (no caso da AWS), ou modelo VMware (no caso do VMware) como entrada de perfil de máquina para converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina. Novas VMs adicionadas ao catálogo assumem os valores de propriedade do perfil de máquina.

Nota:

Um catálogo de máquinas existente baseado em perfil de máquina não pode ser alterado para um catálogo de máquinas não baseado em perfil de máquina.

Para fazer isso:

1. Crie um catálogo de máquinas persistente ou não persistente com VMs e sem um perfil de máquina.
2. Abra a janela do **PowerShell**.
3. Execute o comando `Set-ProvScheme` para aplicar os valores de propriedade do perfil da máquina às novas VMs adicionadas ao catálogo de máquinas. Por exemplo:
   - No caso do Azure:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
     \HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
     Name>\<TemplateSpecName>\<VersionName>
     ```

   - No caso da AWS:

```
Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
\HostingUnits\<hosting-unit>\<launch-
template>.launchtemplate\<launch-template-
version>.launchtemplateversion"
```

- No caso do VMware:

```
Set-ProvScheme -ProvisioningSchemeName "my-prov-scheme"
-MachineProfile "XDHyp:\HostingUnits\my-hosting-unit\my-
template.template"
```

> **Nota:**
>
> Defina `FolderID` como a propriedade personalizada para evitar derivar `FolderID` do modelo VMware.

Recuperar avisos e erros associados a um catálogo

Você pode obter erros e avisos históricos para entender os problemas com seu catálogo de máquinas MCS e corrigi-los.

Usando comandos PowerShell, você pode:

- Obter uma lista de erros ou avisos
- Alterar o estado do aviso de **Novo** para **Reconhecido**
- Excluir os erros ou avisos

Para executar os comandos PowerShell:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.

Para obter uma lista de erros e avisos:

Execute o comando `Get-ProvOperationEvent`.

- Sem parâmetros: Obtém todos os erros e avisos

- Com os parâmetros `LinkedObjectType` e `LinkedObjectUid`: Obtém todos os erros e avisos associados a um esquema de provisionamento específico
- Com o parâmetro `EventId`: Obtém um erro ou aviso específico que corresponde a este ID de evento
- Com o parâmetro `Filter`: Obtém erros ou avisos por um filtro personalizado

Para alterar o estado de erros ou avisos de **Novo** para **Reconhecido**:

Execute o comando `Confirm-ProvOperationEvent`.

- Com o parâmetro `EventId`: Define o estado de um erro ou aviso específico que corresponde a este ID de evento. Você pode obter o `EventId` de um erro ou aviso específico como saída do comando `Get-ProvOperationEvent`
- Com os parâmetros `LinkedObjectType` e `LinkedObjectUid`: Define o estado de todos os erros e avisos associados a um esquema de provisionamento específico
- Com o parâmetro `All`: Define o estado de todos os erros e avisos como **Reconhecido**

Para excluir os erros ou avisos:

Execute o comando `Remove-ProvOperationEvent`.

- Com o parâmetro `EventId`: Remove um erro ou aviso específico que corresponde a este ID de evento. Você pode obter o `EventId` de um erro ou aviso específico como saída do comando `Get-ProvOperationEvent`.
- Com os parâmetros `LinkedObjectType` e `LinkedObjectUid`: Remove todos os erros e avisos associados a um esquema de provisionamento específico
- Com o parâmetro `All`: Remove todos os erros e avisos

Para obter mais informações, consulte o Citrix PowerShell SDK.

Excluir máquinas sem acesso ao hipervisor

Ao excluir uma VM ou um esquema de provisionamento, o MCS precisa remover tags da VM e, às vezes, também do disco base, para que os recursos incluídos nas opções de exclusão não sejam mais rastreados ou identificados pelo MCS. No entanto, alguns desses recursos são acessíveis apenas através do hipervisor. Use a opção `PurgeDBOnly` no PowerShell `Remove-ProvVM` para excluir objetos de recurso de VM, como VM, disco base, imagem no ACG e assim por diante, do banco de dados, mesmo quando não há acesso ao hipervisor.

Esta opção está habilitada em:

- todos os hipervisores suportados
- VMs persistentes e não persistentes

Limitações

Você não pode usar os comandos -PurgeDBOnly e -ForgetVM ao mesmo tempo.

Usar o comando PurgeDBOnly

Ao executar o comando PowerShell `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM`, a operação de exclusão pode falhar nos seguintes cenários:

- A conexão do host está em modo de manutenção
- Credenciais inválidas
- Falha na autenticação
- Operação não autorizada
- O hipervisor está inacessível

> **Nota:**

> Remove-provVM -ForgetVM tem como alvo apenas VMs persistentes. Se uma das VMs na lista não for persistente, a operação falhará.

> Quando a operação falha porque o hipervisor está inacessível, o seguinte prompt aparece:

`Try to use -PurgeDBOnly option to clean DDC database.`.

Use a opção `-PurgeDBOnly` no comando PowerShell `Remove-ProvVM` para excluir referências de uma VM do banco de dados MCS. Por exemplo,

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -PurgeDBOnly
```

Atualizar propriedades de VMs individuais

Você pode atualizar as propriedades de VMs individuais em um catálogo de máquinas MCS persistente usando o comando PowerShell `Set-ProvVM`. No entanto, as atualizações não são aplicadas imediatamente. Você deve definir a janela de tempo usando o comando PowerShell `Set-ProvVMUpdateTimeWindow` para que as atualizações sejam aplicadas.

Esta implementação ajuda você a gerenciar VMs individuais de forma eficiente sem atualizar todo o catálogo de máquinas. Atualmente, este recurso é aplicável a ambientes Azure e VMware.

Atualmente, as propriedades que você pode atualizar são:

- `CustomProperties`
- `ServiceOffering` (Não aplicável ao VMware)
- `MachineProfile`
- `CpuCount`
- `Memory`

Usando este recurso, você pode:

- Atualizar as propriedades de uma VM
- Manter as propriedades atualizadas em uma VM após a atualização do catálogo de máquinas
- Reverter as atualizações de configuração aplicadas a uma VM

Antes de atualizar as propriedades de uma VM:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Verifique a configuração do catálogo de máquinas existente. Por exemplo:

   ```
   Get-ProvScheme -ProvisioningSchemeName <catalog name>
   ```

4. Verifique a configuração da VM na qual você deseja aplicar as atualizações. Por exemplo:

   ```
   Get-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
   ```

Atualizar propriedades de uma VM

Faça o seguinte para atualizar as propriedades em uma VM:

1. Desligue a VM na qual você deseja aplicar as atualizações.
2. Atualize as propriedades da VM. Por exemplo, se você quiser atualizar a propriedade personalizada do tipo de armazenamento (`StorageType`) da VM, execute o seguinte:

```
Set-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

Você pode atualizar as propriedades de duas VMs em um catálogo de máquinas simultaneamente. Por exemplo:

```
Set-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

Nota:

As atualizações não são aplicadas imediatamente.

3. Obtenha a lista de propriedades que devem ser atualizadas e a versão da configuração. Por exemplo:

   ```
   Get-ProvVMConfiguration -ProvisioningSchemeName <catalog name> -VMName
   machine1
   ```

   Verifique o valor da propriedade de `Version` e as propriedades a serem atualizadas (neste caso, `StorageType`).

4. Verifique a versão da configuração. Por exemplo:

   ```
   Get-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
   ```

   Verifique o valor da propriedade de `ProvVMConfigurationVersion`. A atualização ainda não foi aplicada. A VM ainda está na configuração antiga.

5. Solicite a atualização agendada. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <catalog name>
-StartsNow -DurationInMinutes -1
```

Para obter mais informações sobre atualizações agendadas, consulte Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento.

> **Nota:**
>
> Qualquer atualização pendente do esquema de provisionamento também é aplicada.

6. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. Verifique a versão da configuração. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

   Verifique o valor da propriedade de `ProvVMConfigurationVersion`. A atualização agora foi aplicada. A VM agora tem a nova configuração.

8. Para aplicar mais atualizações de configuração na VM, desligue a VM e repita os passos.

Manter as propriedades atualizadas em uma VM após a atualização do catálogo de máquinas

Faça o seguinte para manter as propriedades atualizadas em uma VM:

1. Desligue a VM na qual você deseja aplicar as atualizações.
2. Atualize o catálogo de máquinas. Por exemplo, se você quiser alterar o tamanho da VM (`ServiceOffering`) e o tipo de armazenamento (`StorageType`), execute o seguinte:

```
Set-ProvScheme -ProvisioningSchemeName <catalog name> -ServiceOffering
Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

3. Obtenha os detalhes de configuração do catálogo de máquinas. Por exemplo:

```
Get-ProvScheme -ProvisioningSchemeName <catalog name>
```

O `ProvisioningSchemeVersion` agora é incrementado em um. O tamanho da VM e o tipo de armazenamento também são atualizados.

4. Atualize as propriedades da VM. Por exemplo, forneça um perfil de máquina para a VM.

```
Set-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
spec>.templatespec\<template-spec-version>.templatespecversion"
```

> **Nota:**
>
> A entrada do perfil da máquina tem uma tag e um tamanho de VM diferente (`ServiceOffering`) especificado.

5. Obtenha a lista de propriedades que a VM terá após mesclar as atualizações de configuração na VM com as atualizações do catálogo de máquinas. Por exemplo:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName <catalog
name> -VMName machine1
```

> **Nota:**
>
> Quaisquer atualizações na VM substituirão as atualizações feitas no catálogo de máquinas.

6. Solicite atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <catalog name>
-VMName machine1 -StartsNow -DurationInMinutes -1
```

7. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

A VM mantém seu tamanho de VM atualizado conforme derivado do perfil da máquina. Os valores de tag especificados no perfil da máquina também são aplicados à VM. No entanto, o tipo de armazenamento é derivado do esquema de provisionamento mais recente.

8. Obtenha a versão de configuração da VM. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
```

O `ProvisioningSchemeVersion` e o `ProvVMConfigurationVersion` agora mostram a versão mais recente.

Reverter as atualizações de configuração aplicadas a uma VM

1. Após aplicar as atualizações a uma VM, desligue a VM.
2. Execute o seguinte comando para remover as atualizações aplicadas na VM. Por exemplo:

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
<catalog name> -VMName machine1
```

3. Solicite a atualização agendada para a VM. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <catalog name>
-VMName machine1 -StartsNow -DurationInMinutes -1
```

4. Reinicie a VM. Por exemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. Verifique a versão de configuração da VM. Por exemplo:

```
Get-ProvVM -ProvisioningSchemeName <catalog name> -VMName machine1
```

O valor `ProvVMConfigurationVersion` agora é a versão de configuração do catálogo de máquinas.

Migração de armazenamento de VMs

Você pode mover o armazenamento em disco de VMs existentes de um armazenamento antigo para um novo armazenamento em ambientes VMware e XenServer. Durante a migração, o MCS retém os recursos da VM, como gerenciamento de energia, redefinição do disco do SO e assim por diante. Você também pode adicionar novas VMs ao catálogo de máquinas usando o novo armazenamento em disco. Para fazer isso, use o comando PowerShell `Move-ProvVMDisk`.

Você pode migrar VMs persistentes de clone completo e VMs não persistentes.

- Para VMs persistentes de Clone Completo: Disco do SO, Disco de Identidade e discos provisionados não-MCS.
- Para VMs não persistentes: Disco do SO, Disco de Identidade e disco de Cache de Write-back (WBC).

O novo armazenamento deve satisfazer as seguintes condições:

- Deve estar dentro do mesmo cluster do armazenamento antigo.
- O host no qual a VM está sendo executada deve ter acesso aos datastores antigo e novo.

Migrar o armazenamento em disco

Para migrar o armazenamento em disco:

1. Adicione um armazenamento de destino a uma unidade de hospedagem existente. Você pode executar o comando PowerShell `Add-Hyphostingunitstorage` para adicionar o armazenamento de destino:

   Se você não quiser adicionar novas VMs ao armazenamento antigo, altere o armazenamento antigo para **Substituído**. Você pode fazer isso usando o Studio ou comandos PowerShell. Para o Studio, consulte Editar armazenamento. Alternativamente, execute `Set-Hyphostingunitstorage` e defina `Superseded` como `true` para desabilitar a criação de novas VMs no armazenamento antigo.

   > **Nota:**
   >
   > Para VMs não persistentes:

- Se o WBC for usado, configure o armazenamento de destino do WBC na unidade de hospedagem.
- Se o armazenamento de destino do SO estiver configurado, o WBC (se usado) deve ser compatível com o armazenamento de destino do SO.
- Se o armazenamento de destino do SO não estiver configurado, o WBC (se usado) deve ser compatível com o armazenamento do SO atual.

2. Desligue as VMs e ative o **Modo de Manutenção**.
3. Obtenha as informações sobre o esquema de provisionamento, unidade de hospedagem, armazenamento em disco do SO e armazenamento em disco do WBC.

   - Execute `ProvResourceInStorage` para obter informações de armazenamento do SO. Por exemplo:

     ```
     $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
     xxxxx

     $result

     $result.ProvResourceInStorage | Format-List -Property *
     ```

   - Execute `TemporaryStorageInfo` para informações de armazenamento WBC. Por exemplo:

     ```
     $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
     xxxxx

     $result

     $result.TemporaryStorageInfo | Format-List -Property *
     ```

4. Migre o disco do SO, o disco de Identidade e o disco WBC (aplicável a VMs não persistentes) para o armazenamento de destino usando o comando PowerShell `Move-ProvVMDisk`.

Nota:

- Sempre forneça os discos do SO e de Identidade nos parâmetros DiskType e `DestinationStorageId`.
- O `DestinationStorageId` para o disco do SO e o disco de Identidade deve ser o mesmo.

Exemplo:

VMs persistentes:

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myFullCloneProvScheme" -VMName "machine01"
-DiskType OS,Identity -DestinationStorageId datastore1,datastore1
```

Importante:

Para VMs persistentes, todos os discos são movidos. Não é possível selecionar quais discos mover.

VMs não persistentes:

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myCleanOnBootProvScheme" -VMName "machine01"
-DiskType OS,Identity,WBC -DestinationStorageId None,None,datastore1
```

Importante:

- Se você não quiser migrar um disco específico, defina o valor como `None` para o parâmetro `DestinationStorageId`.
- Se a VM tiver um disco WBC, adicione o disco WBC no parâmetro `DiskType` e adicione as informações necessárias no parâmetro `DestinationStorageId`.

Solução de problemas

Se um dos discos falhar ao migrar, nenhum dos discos será migrado para o armazenamento de destino. Você pode obter o relatório de falha usando o seguinte comando:

```
(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines
```

Considerações importantes para a migração de VMs não persistentes no VMware

- Se você tentar mover o disco do SO e de Identidade para um novo armazenamento, os arquivos específicos da VM também serão movidos para o novo armazenamento.
- O VMware não oferece suporte à movimentação do disco se ele tiver o snapshot.

Migrar catálogos provisionados por MCS existentes para um catálogo de máquinas de imagem preparada

Você pode converter um catálogo de máquinas provisionado por MCS existente em um catálogo de máquinas de imagem preparada usando um comando PowerShell `Set-ProvSchemeImage`. No entanto, você não pode reverter para o catálogo herdado após a migração. Atualmente, esse recurso é aplicável a ambientes de virtualização Azure e VMware.

Limitações

Considere as seguintes limitações:

- Se o catálogo MCS usar um disco de dados persistente, o catálogo não poderá ser migrado para usar uma imagem preparada.
- Se o catálogo MCS usar discos não gerenciados, o catálogo não poderá ser migrado para usar uma imagem preparada.

Migrar para o catálogo de máquinas de imagem preparada

Para migrar, faça o seguinte:

1. Crie uma definição de imagem e versões de imagem usando comandos do Studio ou PowerShell. Consulte as etapas para criar definições de imagem e versões de imagem em:
    - Azure:
        - Studio
        - PowerShell

- VMware:
  - Studio
  - PowerShell

2. Execute o comando `Get-ProvScheme` para obter o UID do esquema de provisionamento. Por exemplo:

```
Get-ProvScheme -ProvisioningSchemeName <name> | select
ProvisioningSchemeName, ProvisioningSchemeUid
```

3. Execute o comando `Get-ProvImageVersionSpec` para obter o nome da definição da imagem, o UID da especificação da versão da imagem. Por exemplo:

```
Get-ProvImageVersionSpec -ImageDifinitionName <name> -Filter
{IsPrepared -eq $true} | select ImageDefinitionName ImageVersionSpecUId
```

4. Execute o comando `Set-ProvSchemeImage` para migrar um catálogo de máquinas provisionado pelo MCS existente para um catálogo de máquinas de imagem preparada. Por exemplo:

```
Set-ProvSchemeImage -ProvisioningSchemeName [ProvisioningSchemeName]
-ImageVersionSpecUid [ImageVersionSpecUid]
```

5. Execute o comando `Get-ProvScheme` para verificar se o catálogo foi migrado. Por exemplo:

```
Get-ProvScheme -ProvisioningSchemeName <name> | select
ProvisioningSchemeName, ProvisioningSchemeUid, ImageVersionSpecUid
```

Solução de problemas

- Para máquinas com status `Power State Unknown`, consulte CTX131267 para obter orientação.
- Para corrigir VMs que exibem continuamente um estado de energia desconhecido, consulte Como corrigir VMs que exibem continuamente um estado de energia desconhecido.
- Se um Cloud Connector não estiver funcionando corretamente, as operações de provisionamento do MCS (como atualizações de catálogo) demoram mais do que o normal e o desempenho do console de gerenciamento degrada significativamente.

Onde ir em seguida

Para obter informações sobre como gerenciar catálogos de hipervisor específicos, consulte:

- Gerenciar um catálogo AWS
- Gerenciar um catálogo do Google Cloud Platform
- Gerenciar um catálogo do Microsoft Azure
- Gerenciar um catálogo do Microsoft System Center Virtual Machine Manager
- Gerenciar um catálogo do VMware
- Gerenciar um catálogo do XenServer

Gerenciar um catálogo AWS EC2

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de nuvem AWS EC2.

> **Nota:**
>
> Antes de gerenciar um catálogo AWS, você precisa terminar de criar um catálogo AWS. Consulte Criar um catálogo AWS EC2.

Remover tags

Ao criar um catálogo ou uma VM, as tags são criadas nos seguintes recursos:

- Máquina virtual
- Volume do disco raiz
- Volume do disco de identidade
- Interface de rede elástica (ENI)
- Imagem do disco raiz (AMI)
- Modelo de inicialização
- Snapshot de AMI ou disco raiz

Você pode remover VMs e catálogos de máquinas do banco de dados Citrix® e remover tags criadas pelo Citrix. Você pode usar:

- `Remove-ProvVM` com o parâmetro `ForgetVM` para remover VMs e tags criadas pelo Citrix de uma única VM ou de uma lista de VMs de um catálogo de máquinas.

  > **Nota:**
  >
  > Com o parâmetro `ForgetVM`, as VMs são removidas do banco de dados do esquema de provisionamento da Citrix; no entanto, as VMs continuam a permanecer no hipervisor.

- `Remove-ProvScheme` com o parâmetro `ForgetVM` para remover um catálogo de máquinas do banco de dados da Citrix e recursos de um catálogo de máquinas.

Para fazer isso:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Desbloqueie a VM antes de remover as VMs. Por exemplo:

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. Execute um dos seguintes comandos para remover VMs, catálogo de máquinas e tags criadas pela Citrix dos recursos.

   - Execute `Remove-ProvVM` com `ForgetVM` para remover VMs do banco de dados da Citrix e tags criadas pela Citrix das VMs. Por exemplo:

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
     -ForgetVM
     ```

   - Execute `Remove-ProvScheme` para remover o catálogo de máquinas do banco de dados da Citrix e recursos de um catálogo de máquinas. Por exemplo:

     ```
     Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
     ```

5. Verifique se a VM foi removida do Delivery Controller™, mas não do hipervisor.

   a. Execute `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`. Isso não deve retornar nada.

b. Vá para o console do AWS EC2. Você deve ver as VMs; no entanto, as tags criadas pela Citrix foram removidas. As tags criadas pela Citrix dos seguintes recursos são removidas:

- Máquina virtual
- Volume de disco raiz
- Volume do disco de identidade
- ENI

6. Se você remover o catálogo de máquinas, verifique se o catálogo foi removido do Delivery Controller.

a. Execute `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`. Isso deve retornar um erro.

b. Verifique no console do AWS EC2 se os seguintes recursos foram removidos.

- Imagem do disco raiz (AMI)
- Modelo de inicialização
- Snapshot da AMI ou do disco raiz

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos na plataforma AWS. As tags na tabela são representadas como "chave":"valor".

NOME DO RECURSO	TAG
Disco de ID	"Name": "VMName_IdentityDisk"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Imagem	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ENI	"Description": "XD Nic"
	"XdConfig": "XdProvisioned=true"

NOME DO RECURSO	TAG
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco do SO	"Name": "VMName_rootDisk"
	"XdConfig": "XdProvisioned=True"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Recurso Citrix": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
PrepVM	"Nome": "Preparação - CatalogName - xxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Recurso Citrix": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
Instantâneo publicado	"XdConfig": "XdProvisioned=true"
	Se não for um instantâneo para Volume Worker AMI, então "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Modelo	[when AwsCaptureInstanceProperties = true] "XdConfig": "XdProvisioned=true"

NOME DO RECURSO	TAG
	[when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
VM no catálogo	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx"
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
AMI do trabalhador de volume	"XdConfig": "XdProvisioned=true"
Bootstraper do trabalhador de volume	"Name": "XenDesktop® Temp"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": ""

NOME DO RECURSO	TAG
Instância do trabalhador de volume	"Name": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx"
	"XdConfig": "XdProvisioned=true"

Converter catálogos MCS legados na AWS para catálogos baseados em perfil de máquina

Para converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina, conclua as seguintes etapas:

1. Na página **Catálogos de Máquinas**, clique com o botão direito do mouse no nome do **Catálogo de Máquinas** que você deseja converter e selecione **Editar Catálogo de Máquinas**.
2. Na página **Editar Catálogo de Máquinas > Perfil de Máquina**, marque a caixa de seleção **Usar um perfil de máquina**.
3. Clique em **Selecionar um perfil de máquina**.
4. Na página **Selecionar um perfil de máquina**, selecione uma máquina virtual ou um modelo de inicialização para usar como perfil de máquina.
5. Se algumas configurações atuais diferirem das novas configurações de perfil de máquina, selecione a opção necessária para as configurações que deseja usar e clique em **Continuar**.
6. Clique em **Aplicar**.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o AWS EC2
- Criar catálogos de máquinas
- Criar um catálogo AWS EC2
- Gerenciar catálogos de máquinas

Gerenciar um catálogo de instâncias gerenciadas do Amazon WorkSpaces Core

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos das instâncias gerenciadas do Amazon WorkSpaces Core.

> **Nota:**
>
> Antes de gerenciar um catálogo de instâncias gerenciadas do Amazon WorkSpaces Core, você precisa concluir a criação de um catálogo de instâncias gerenciadas do Amazon WorkSpaces Core. Consulte Criar um catálogo de instâncias gerenciadas do Amazon WorkSpaces Core.

Remover tags

Ao criar um catálogo ou uma VM, as tags são criadas nos seguintes recursos:

- Máquina virtual
- Volume do disco raiz
- Volume do disco de identidade
- Interface de rede elástica (ENI)
- Imagem do disco raiz (AMI)
- Modelo de inicialização
- Snapshot de AMI ou disco raiz

Você pode remover VMs e catálogos de máquinas do banco de dados Citrix® e remover tags criadas pelo Citrix. Você pode usar:

- `Remove-ProvVM` com o parâmetro `ForgetVM` para remover VMs e tags criadas pelo Citrix de uma única VM ou de uma lista de VMs de um catálogo de máquinas.

  > **Nota:**
  >
  > Com o parâmetro `ForgetVM`, as VMs são removidas do banco de dados do esquema de provisionamento da Citrix; no entanto, as VMs continuam a permanecer no hipervisor.

- `Remove-ProvScheme` com o parâmetro `ForgetVM` para remover um catálogo de máquinas do banco de dados da Citrix e recursos de um catálogo de máquinas.

Para fazer isso:

1. Abra uma janela do **PowerShell**.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Desbloqueie a VM antes de remover as VMs. Por exemplo:

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
```

4. Execute um dos seguintes comandos para remover VMs, catálogo de máquinas e tags criadas pela Citrix dos recursos.

   - Execute `Remove-ProvVM` com `ForgetVM` para remover VMs do banco de dados da Citrix e tags criadas pela Citrix das VMs. Por exemplo:

```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
-ForgetVM
```

   - Execute `Remove-ProvScheme` para remover o catálogo de máquinas do banco de dados da Citrix e recursos de um catálogo de máquinas. Por exemplo:

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
```

5. Verifique se a VM foi removida do Delivery Controller™, mas não do hipervisor.

   a. Execute `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`. Isso não deve retornar nada.

   b. Vá para o console do AWS EC2. Você deve ver as VMs; no entanto, as tags criadas pela Citrix foram removidas. As tags criadas pela Citrix dos seguintes recursos são removidas:

      - Máquina virtual
      - Volume do disco raiz
      - Volume do disco de identidade
      - ENI

6. Se você remover o catálogo de máquinas, verifique se o catálogo foi removido do Delivery Controller.

    a. Execute `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`. Isso deve retornar um erro.

    b. Verifique no console do AWS EC2 se os seguintes recursos foram removidos.

    - Imagem do disco raiz (AMI)
    - Modelo de inicialização
    - Snapshot da AMI ou do disco raiz

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos na plataforma AWS. As tags na tabela são representadas como "chave":"valor".

NOME DO RECURSO	TAG
Disco de ID	"Name": "VMName_IdentityDisk"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Imagem	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ENI	"Description": "XD Nic"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco do SO	"Name": "VMName_rootDisk"
	"XdConfig": "XdProvisioned=True"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

NOME DO RECURSO	TAG
PrepVM	"Nome": "Preparação - Nome do Catálogo - xxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Instantâneo publicado	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Modelo	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM no catálogo	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Mais informações

- Ambientes de virtualização AWS
- Conexão com instâncias gerenciadas do Amazon WorkSpaces Core
- Gerenciamento de imagens
- Criar uma imagem preparada para instâncias gerenciadas do Amazon WorkSpaces Core
- Criar um catálogo de instâncias gerenciadas do Amazon WorkSpaces Core
- Gerenciar catálogos de máquinas de imagem preparada

Gerenciar um catálogo do Google Cloud Platform

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de nuvem do Google.

> **Nota:**
>
> Antes de gerenciar um catálogo do Google Cloud Platform, você precisa terminar de criar um catálogo do Google Cloud Platform. Consulte Criar um catálogo do Google Cloud Platform.

Adicionar máquinas a um catálogo

Para adicionar máquinas a um catálogo, siga estas etapas:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione o catálogo de máquinas ao qual você deseja adicionar máquinas.
3. Selecione **Adicionar Máquinas** na barra de ações.
4. Na página **Máquinas Virtuais**, especifique o número de máquinas que você deseja adicionar e, em seguida, selecione **Avançar**.
5. Na página **Identidades da Máquina**, selecione uma conta do Active Directory e, em seguida, selecione **Avançar**.
6. Na página **Credenciais de Domínio**, selecione **Inserir credenciais**, digite o nome de usuário e a senha, selecione **Salvar** e, em seguida, selecione **Avançar**.
7. Na página **Resumo**, confirme as informações e, em seguida, selecione **Concluir**.

Atualizar máquinas

Este recurso pode ser útil em casos em que você deseja atualizar sua imagem mestre ou o nível funcional mínimo.

Para atualizar máquinas, siga estas etapas:

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione o catálogo de máquinas que contém as máquinas que você deseja atualizar.
3. Selecione **Alterar Imagem Mestra** na barra de ações.
4. Na página **Imagem**, selecione uma VM e o nível funcional mínimo para o catálogo e, em seguida, selecione **Avançar**.
5. Na página **Estratégia de Implantação**, especifique quando você deseja atualizar as máquinas e, em seguida, selecione **Avançar**.
6. Na página **Resumo**, confirme as informações e, em seguida, selecione **Concluir**.

Reverter uma atualização de máquina

Para reverter uma atualização de máquina, siga estas etapas:

> **Importante:**
>
> Não renomeie, exclua ou mova imagens mestras. Caso contrário, você não poderá reverter a atualização.

1. No Studio, selecione **Catálogos de Máquinas** no painel esquerdo.
2. Selecione o catálogo de máquinas onde você deseja reverter a atualização da máquina.
3. Selecione **Reverter Imagem Mestra** na barra de ações.
4. Na página **Visão Geral**, confirme as informações e, em seguida, selecione **Avançar**.
5. Na página **Estratégia de Implantação**, configure a estratégia de implantação e selecione **Avançar**.
6. Na página **Resumo**, confirme as informações e selecione **Concluir**.

Gerenciamento de energia

O Citrix DaaS™ permite gerenciar a energia das máquinas do Google Cloud. Use o nó **Pesquisar** no painel de navegação para localizar a máquina que você deseja gerenciar a energia. As seguintes ações de energia estão disponíveis:

- Excluir
- Iniciar
- Reiniciar
- Forçar Reinício
- Desligar
- Forçar Desligamento
- Adicionar ao Grupo de Entrega
- Gerenciar Tags
- Ativar Modo de Manutenção

Você também pode gerenciar a energia das máquinas do Google Cloud usando o Autoscale. Para fazer isso, adicione as máquinas do Google Cloud a um Grupo de Entrega e, em seguida, ative o

Autoscale para esse Grupo de Entrega. Para obter mais informações sobre o Autoscale, consulte Autoscale.

Atualizar máquinas provisionadas usando PowerShell

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, ele não afeta as máquinas existentes. Usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`, agora você pode aplicar o esquema de provisionamento atual a uma máquina ou conjunto de máquinas persistentes ou não persistentes existentes. Atualmente, no GCP, as atualizações de propriedade suportadas por esse recurso são Perfil da máquina, Oferta de serviço e Configurações de catálogo personalizadas.

Você pode atualizar:

- Uma única VM
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um ID de esquema de provisionamento
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um nome de esquema de provisionamento

Para atualizar as VMs existentes:

1. Verifique a configuração das máquinas existentes. Por exemplo,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. Atualize o esquema de provisionamento. Por exemplo,

   - Atualizando o perfil da máquina

     ```
     `Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
     "XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
     ```

   - Atualizando a oferta de serviço

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
     “XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
     offering>.serviceoffering"
     ```

3. Verifique se a propriedade atual da VM corresponde ao esquema de provisionamento atual e se há alguma ação de atualização pendente na VM. Por exemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

   Você também pode encontrar máquinas com uma versão específica. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

4. Atualize as máquinas existentes.

   - Para atualizar todas as máquinas existentes:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

   - Para atualizar uma lista de máquinas específicas:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

   - Para atualizar máquinas com base na saída de `Get-ProvVM`:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

   Nota:

   - `StartsNow` indica que a hora de início agendada é a hora atual.
   - `DurationInMinutes` com um número negativo (por exemplo, –1) indica que não há limite superior na janela de tempo do agendamento.

5. Encontre máquinas com uma atualização agendada. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

6. Reinicie as máquinas. No próximo ligar, as alterações de propriedade são aplicadas às máquinas existentes. Você pode verificar o status atualizado usando o seguinte comando:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

Alterar propriedades personalizadas relacionadas ao disco de um catálogo existente

Você pode alterar as seguintes propriedades personalizadas relacionadas ao disco de um catálogo existente e de VMs existentes do catálogo:

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

Nota:

- A propriedade `StorageType` é para o disco do SO
- A propriedade `PersistOsDisk` pode ser definida apenas para catálogos não persistentes com cache de write-back ativado.

Esta implementação ajuda você a selecionar diferentes tipos de armazenamento para diferentes discos mesmo após a criação de um catálogo e, assim, equilibra os preços associados aos diferentes tipos de armazenamento.

Para fazer isso, use os comandos do PowerShell `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`:

1. Abra uma janela do **PowerShell**.

2. Execute `asnp citrix*`.
3. Execute `Get-ProvVM -VMName <VM name>` para obter as propriedades personalizadas.
4. Altere a string de propriedades personalizadas:
    a. Copie as propriedades personalizadas para um Bloco de Notas e altere as propriedades personalizadas.
    b. Na janela do **PowerShell**, cole as propriedades personalizadas modificadas do Bloco de Notas e atribua uma variável às propriedades personalizadas modificadas. Por exemplo:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. Atualize o catálogo existente. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. Atualize as VMs existentes. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. Reinicie as VMs. Na próxima inicialização, as alterações de propriedade personalizadas são aplicadas às VMs existentes.

Proteger contra exclusão acidental de máquina

O Citrix DaaS permite proteger os recursos do MCS no Google Cloud para evitar exclusão acidental. Configure a VM provisionada definindo o sinalizador `deletionProtection` como TRUE.

Por padrão, as VMs provisionadas por meio do plug-in MCS ou Google Cloud são criadas com o InstanceProtection ativado. A implementação é aplicável a catálogos persistentes e não persistentes. Os catálogos não persistentes são atualizados quando as instâncias são recriadas a partir do modelo. Para máquinas persistentes existentes, você pode definir o sinalizador no console do Google Cloud. Para obter mais informações sobre como definir o sinalizador, consulte o site de Documentação do Google. Novas máquinas adicionadas a catálogos persistentes são criadas com `deletionProtection` ativado.

Se você tentar excluir uma instância de VM para a qual você definiu o sinalizador `deletionProtection`, a solicitação falhará. No entanto, se você tiver a permissão `compute.instances.setDeletionProtection` ou for atribuído à função IAM de **Administrador de Computação**, você pode redefinir o sinalizador para permitir que o recurso seja excluído.

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos na plataforma GCP. As tags na tabela são representadas como "chave":"valor".

NOME DO RECURSO	TAG
Disco de ID	"CitrixResource": "interno"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Imagem	"CitrixResource": "interno"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco do SO	"CitrixResource": "interno"

NOME DO RECURSO	TAG
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM de preparação	"CitrixResource": "interno"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Instantâneo publicado	"CitrixResource": "interno"
Bucket de armazenamento	"CitrixResource": "interno"
Modelo	"CitrixResource": "interno"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM no catálogo	"CitrixResource": "interno"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx". O plug-in também adiciona este rótulo para VMs provisionadas pelo MCS: "citrix-provisioning-scheme-id": "provSchemeId". Você pode usar este rótulo para filtrar por catálogo no console do GCP.
Disco WBC	"CitrixResource": "interno"
	CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Nota:

Uma VM não fica visível no inventário do Citrix se uma tag **CitrixResource** for adicionada para identificá-la como um recurso criado pelo MCS. Você pode remover ou renomear a tag para torná-la visível.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com ambientes de nuvem do Google
- Criar catálogos de máquinas
- Criar um catálogo do Google Cloud Platform
- Gerenciar catálogos de máquinas

Gerenciar um catálogo HPE Moonshot

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos do catálogo HPE Moonshot.

> **Nota:**
>
> Antes de gerenciar um catálogo HPE Moonshot, você precisa concluir a criação de um catálogo HPE Moonshot. Consulte Criar um catálogo de máquinas HPE Moonshot.

Gerenciamento de energia

O Citrix DaaS™ permite que você faça o gerenciamento de energia de máquinas HPE Moonshot. Use o nó **Pesquisar** no painel de navegação para localizar a máquina que você deseja gerenciar. As seguintes ações de energia estão disponíveis:

- Iniciar
- Desligar
- Desligamento Forçado
- Reiniciar
- Redefinir

> **Nota:**
>
> As ações de energia **Suspender** e **Retomar** não são suportadas.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com HPE Moonshot
- Criar catálogos de máquinas
- Criar um catálogo de máquinas HPE Moonshot
- Gerenciar catálogos de máquinas

Gerenciar um catálogo do Microsoft Azure

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de nuvem do Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de gerenciar um catálogo do Microsoft Azure, você precisa concluir a criação de um catálogo do Microsoft Azure. Consulte Criar um catálogo do Microsoft Azure.

Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada

Você pode economizar custos de armazenamento alterando o tipo de armazenamento de um disco gerenciado para um nível inferior ao desligar uma VM. Para fazer isso, use a propriedade personalizada `StorageTypeAtShutdown`.

O tipo de armazenamento do disco muda para um nível inferior (conforme especificado na propriedade personalizada `StorageTypeAtShutdown`) quando você desliga a VM. Depois de ligar a VM, o tipo de armazenamento volta ao original (conforme especificado na propriedade personalizada `StorageType` ou na propriedade personalizada `WBCDiskStorageType`).

> **Importante:**
>
> - O disco não existe até que a VM seja ligada pelo menos uma vez. Portanto, você não pode alterar o tipo de armazenamento ao ligar a VM pela primeira vez.
> - Uma VM pode demorar um pouco mais para iniciar depois que você altera o tipo de armazenamento para um nível inferior.

Requisitos

- Aplicável a um disco gerenciado. Isso implica que você define a propriedade personalizada `UseManagedDisks` como true.
- Aplicável a um catálogo persistente e não persistente com um disco de SO persistente. Isso implica que você define a propriedade personalizada `persistOsDisk` como true.
- Aplicável a um catálogo não persistente com um disco WBC persistente. Isso implica que você define a propriedade personalizada `persistWBC` como true.

Restrição

- De acordo com a Microsoft, você só pode alterar o tipo de disco duas vezes por dia. Consulte o documento da Microsoft. De acordo com a Citrix, a atualização `StorageType` ocorre sempre que há uma ação de Iniciar ou Desalocar para a VM. Portanto, limite o número de ações de energia por VM a duas por dia. Por exemplo, uma ação de energia pela manhã para iniciar a VM e uma à noite para desalocar a VM.

Alterar o tipo de armazenamento para um nível inferior

Antes de prosseguir com as etapas, consulte os Requisitos e as Restrições.

1. Adicione a propriedade personalizada `StorageTypeAtShutdown`, defina o valor como Standard_LRS (HDD) e crie um catálogo usando `New-ProvScheme`.

   > **Nota:**
   >
   > Se `StorageTypeAtShutdown` tiver qualquer valor diferente de vazio ou Standard_LRS (HDD), a operação falha.

   > Exemplo de configuração de propriedades personalizadas ao criar um catálogo persistente:

   ```
   $customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
   2014/xd/machinecreation"

   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

   <Property xsi:type="StringProperty" Name="UseManagedDisks"
   Value="true" />
   ```

```
<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS“ />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>’
```

Exemplo de configuração de propriedades personalizadas ao criar um catálogo não persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
```

```
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>’
```

Nota:

Ao usar um perfil de máquina, a propriedade personalizada tem precedência sobre a propriedade definida em `MachineProfile`.

2. Desligue a VM e verifique o tipo de armazenamento da VM no portal do Azure. O tipo de armazenamento do disco muda para um nível inferior, conforme especificado na propriedade personalizada `StorageTypeAtShutdown`.
3. Ligue a VM. O tipo de armazenamento do disco volta para o tipo de armazenamento mencionado em:
   - propriedade personalizada `StorageType` para disco do SO
   - propriedade personalizada `WBCDiskStorageType` para disco WBC somente se você especificá-lo em `CustomProperties`. Caso contrário, ele volta para o tipo de armazenamento mencionado em `StorageType`.

Aplicar `StorageTypeAtShutdown` a um catálogo existente

Antes de prosseguir com as etapas, consulte os Requisitos e as Restrições.

Use `Set-ProvScheme` para aplicar `StorageTypeAtShutdown` às novas VMs adicionadas a um catálogo existente.

Exemplo de como definir propriedades personalizadas ao adicionar uma VM a um catálogo existente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>’



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName



Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

Altere o tipo de armazenamento de VMs existentes para um nível inferior no desligamento

Antes de prosseguir com as etapas, consulte os Requisitos e as Restrições.

Você pode economizar custos de armazenamento alterando o tipo de armazenamento de VMs existentes para um nível inferior quando as VMs são desligadas.

Para alterar o tipo de armazenamento de máquinas existentes em um catálogo para um nível inferior quando as VMs são desligadas:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Execute `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Altere a string de propriedades personalizadas.

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

5. Atualize o esquema de provisionamento do catálogo existente. A atualização se aplica a novas VMs adicionadas após a execução de `Set-ProvScheme`.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
$customProperties
```

6. Atualize as VMs existentes para habilitar `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

7. Na próxima vez que você ligar as máquinas, a propriedade `StorageTypeAtShutdown` das máquinas será atualizada. O tipo de armazenamento muda no próximo desligamento.
8. Execute o seguinte comando para visualizar o valor `StorageTypeAtShutdown` para cada VM em um catálogo.

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
```

```
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

Converter catálogos MCS legados no Azure para catálogos baseados em perfil de máquina

Para converter um catálogo de máquinas não baseado em perfil de máquina para um catálogo de máquinas baseado em perfil de máquina, conclua as seguintes etapas:

1. Na página **Catálogos de Máquinas**, clique com o botão direito do mouse no nome do **Catálogo de Máquinas** que você deseja converter e selecione **Editar Catálogo de Máquinas**.
2. Na página **Editar Catálogo de Máquinas** > **Perfil da Máquina**, selecione a caixa de seleção **Usar um perfil de máquina (obrigatório para Microsoft Entra ID)**.
3. Clique em **Selecionar um perfil de máquina**.
4. Na página **Selecionar um perfil de máquina**, selecione uma máquina virtual ou um modelo de inicialização para usar como perfil de máquina.
5. Se algumas configurações atuais diferirem das novas configurações de perfil de máquina, selecione a opção necessária para as configurações que você deseja usar e clique em **Continuar**.
6. Clique em **Aplicar**.

Atualizar máquinas provisionadas para o estado atual do esquema de provisionamento

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, ele não afeta as máquinas existentes. Usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`, você pode aplicar o esquema de provisionamento atual a uma máquina ou conjunto de máquinas existente, persistente ou não persistente. Você também pode agendar um período de tempo para as atualizações de configuração das máquinas provisionadas MCS existentes. Qualquer inicialização ou reinicialização durante o período de tempo agendado aplica uma atualização de esquema de provisionamento agendada a uma máquina. Atualmente, no Azure, você pode atualizar `ServiceOffering`, `MachineProfile` e as seguintes propriedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`
- `Zones`

Nota:

- Você só pode atualizar as propriedades personalizadas `StorageType`, `WBCDiskStorageType` e `IdentityDiskStorageType` para um catálogo usando disco gerenciado em ambientes Azure.
- Se você executar `Set-ProvVMUpdateTimeWindow` duas vezes, o comando mais recente terá efeito.
- Se uma VM for atualizada com `Set-ProvVMUpdateTimeWindow` e a lista atual de zonas de disponibilidade fornecida pela propriedade personalizada Zones for alterada para não incluir a zona que a VM está usando atualmente, os discos persistentes da VM serão copiados para a nova zona e os originais serão excluídos. Por exemplo, uma VM provisionada na zona 3 atualizada com a propriedade personalizada Zones definida como “1,2” moverá a VM e seus discos para a zona 1 ou 2, dependendo de qual das duas zonas tem menos máquinas para equilibrar as máquinas entre as zonas 1 e 2.
- Se a propriedade personalizada Zones for totalmente limpa (definida como um valor vazio), a afinidade de zona da VM será removida, permitindo que o Azure coloque a VM em qualquer zona de disponibilidade com base na capacidade. Neste caso, os discos persistentes da VM permanecem em sua zona original e não são movidos.

Você pode atualizar:

- Uma única VM
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um ID de esquema de provisionamento
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um nome de esquema de provisionamento (nome do catálogo de máquinas)

Depois de fazer as seguintes alterações no esquema de provisionamento, a instância da VM é recriada para catálogos persistentes no Azure:

- Alterar o `MachineProfile`
- Remover `LicenseType`
- Remover `DedicatedHostGroupId`

> **Nota:**
>
> O disco do SO das máquinas existentes, juntamente com todos os seus dados, permanece como está e uma nova VM é anexada ao disco.

Antes de atualizar as VMs existentes:

1. Verifique a configuração das máquinas existentes. Por exemplo,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. Atualize o esquema de provisionamento. Por exemplo,

   - Com a VM como entrada de perfil de máquina:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
     "XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<virtual-machine>.vm"
     ```

   - Com a especificação de modelo como entrada de perfil de máquina:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog"

     -MachineProfile "XDHyp:\HostingUnits\<hosting-
     unit>\machineprofile.folder\<resource-
     group>.resourcegroup\<template-spec>.templatespec\<template-spec-
     version>.templatespecversion"
     ```

```
-ServiceOffering "XDHyp:\HostingUnits\<hosting-
unit>\serviceoffering.folder\<service-offering>.serviceoffering"
```

- Apenas com a oferta de serviço:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
"XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
offering>.serviceoffering"
```

3. Verifique se a propriedade atual da VM corresponde ao esquema de provisionamento atual e se há alguma ação de atualização pendente na VM. Por exemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

Você também pode encontrar máquinas com uma versão específica. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

Para solicitar atualizações para máquinas existentes que serão aplicadas na próxima reinicialização:

1. Execute os seguintes comandos para atualizar as máquinas existentes e fazer com que as atualizações sejam aplicadas na próxima reinicialização.

- Para atualizar todas as máquinas existentes. Por exemplo,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

- Para atualizar uma lista de máquinas específicas. Por exemplo,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

- Para atualizar máquinas com base na saída de Get-ProvVM. Por exemplo,

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

Nota:

- `StartsNow` indica que a hora de início agendada é a hora atual.
- `DurationInMinutes` com um número negativo (por exemplo, –1) indica que não há limite superior para a janela de tempo do agendamento.

2. Encontre máquinas com uma atualização agendada. Por exemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. Reinicie as máquinas. No próximo ligamento, as alterações de propriedade são aplicadas às máquinas existentes. Você pode verificar o status atualizado usando o seguinte comando. Por exemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

Para agendar uma VM para atualizar para as configurações de provisionamento mais recentes na próxima vez que ela iniciar na janela de tempo agendada:

1. Execute os seguintes comandos:

   - Para agendar uma atualização com a hora de início como a hora atual:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName vm1 -StartsNow -DurationInMinutes 120
```

   - Para agendar uma atualização em um fim de semana:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
(New –TimeSpan –Days 2).TotalMinutes
```

Nota:

- `VMName` é opcional. Se não for especificado, a atualização é agendada para todo o catálogo.
- Em vez de `StartTimeInUTC`, use `StartsNow` para indicar que a hora de início do agendamento é a hora atual.
- `DurationInMinutes` é opcional. O padrão é 120 minutos. Um número negativo (por exemplo, –1) indica que não há limite superior para a janela de tempo do agendamento.

2. Verifique o status da atualização.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. Ligue a VM. Se você ligar a máquina após o período agendado, a atualização da configuração não será aplicada. Se você ligar a máquina dentro do período agendado,
   - Se a máquina estiver desligada e
     - você não ligar a máquina, a atualização da configuração não será aplicada
     - você ligar a máquina, a atualização da configuração será aplicada
   - Se a máquina estiver ligada e
     - você não reiniciar a máquina, a atualização da configuração não será aplicada
     - você reiniciar a máquina, a atualização da configuração será aplicada

Para cancelar a atualização da configuração:

Você também pode cancelar uma atualização de configuração de uma única VM, de várias VMs ou de um catálogo inteiro. Para cancelar uma atualização de configuração:

1. Execute `Clear-ProvVMUpdateTimeWindow`. Por exemplo:

   - Para cancelar a atualização da configuração agendada para uma única VM:

     ```
     Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
     -VMName “vm1”
     ```

   - Para cancelar a atualização da configuração agendada para várias VMs:

     ```
     Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
     -VMName "vm1","vm2"
     ```

Nota:

As VMs devem ser do mesmo catálogo.

Alterar criptografia de disco

Você pode alterar a criptografia de disco em ambientes de virtualização do Azure e fazer o seguinte:

- Crie um catálogo de máquinas MCS com conjunto de criptografia de disco (DES) que seja diferente do DES da imagem mestre usando o comando `New-ProvScheme`. Por exemplo:

  ```
  $customProperties = @"

  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
  subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/
  providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/
  >

  </CustomProperties>

  "@

  New-ProvScheme -CleanOnBoot `
  ```

```
-ProvisioningSchemeName $provisioningSchemeName `

-HostingUnitName $hostingUnitName `

-IdentityPoolName $identityPoolName `

-InitialBatchSizeHint $numberOfVms `

-masterImagePath $masterImagePath `

-NetworkMapping $networkMapping `

-CustomProperties $customProperties
```

- Altere o tipo de criptografia de disco de uma chave DES para outra chave DES de um catálogo de máquinas MCS existente e VMs existentes usando os comandos `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`. Depois de reiniciar as VMs, você poderá ver a chave DES atualizada. Por exemplo:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- Atualize um catálogo de máquinas MCS e uma VM que não estava anteriormente habilitada para CMEK para ter criptografia de chave de criptografia gerenciada pelo cliente (CMEK) (DES), criptografia de disco no host ou criptografia dupla usando os comandos `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`. Para obter informações sobre os diferentes

tipos de criptografia, consulte Criptografia do lado do servidor do Azure, Criptografia de disco do Azure no host e Criptografia dupla em disco gerenciado.

- Atualize um catálogo de máquinas MCS e VMs existentes para não serem criptografados, que foram criptografados anteriormente usando os comandos `Set-ProvScheme` e `Set-ProvVMUpdateTimeWindow`. Por exemplo:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- Habilite a criptografia de disco com ponto de extremidade privado (um catálogo de máquinas MCS que usou uma conexão de host habilitada com `ProxyHypervisorTrafficThroughConnector`). Para obter mais informações sobre `ProxyHypervisorTrafficThroughConnector`, consulte Criar um ambiente seguro para tráfego gerenciado pelo Azure. Para obter informações sobre como habilitar a criptografia de disco com pontos de extremidade privados, consulte Habilitar criptografia de disco com ponto de extremidade privado.

Habilitar criptografia de disco com ponto de extremidade privado

De acordo com a limitação do Azure, atualmente, você não pode ter criptografia do lado do servidor com chaves gerenciadas pelo cliente para pontos de extremidade privados. No entanto, você pode atualizar um catálogo de máquinas MCS existente e VMs com pontos de extremidade privados para serem criptografados com a chave DES.

ATUALIZAR UM CATÁLOGO DE MÁQUINAS EXISTENTE COM PONTOS DE EXTREMIDADE PRIVADOS

As etapas detalhadas para atualizar um catálogo de máquinas existente com pontos de extremidade privados são as seguintes:

1. Crie um catálogo sem criptografia de disco através de `ProxyHypervisorTrafficThroughConnector`. Para obter mais informações sobre `ProxyHypervisorTrafficThroughConnector`, consulte Criar um ambiente seguro para tráfego gerenciado pelo Azure.
2. Execute `Set-ProvScheme` para atualizar o catálogo com `DiskEncryptionSetId`.

> **Nota:**
>
> `DiskEcryptionSetId` pode ser configurado através de `CustomProperties` ou `MachineProfile`. Quando definido em `CustomProperties` e `MachineProfile`, as propriedades definidas em `CustomProperties` são aplicadas.

Exemplo ao usar `CustomProperties`:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1"/>

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

Exemplo ao usar MachineProfile: Use uma VM com criptografia de disco ativada ou uma especificação de modelo com configurações de criptografia de disco:

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -MachineProfile
"XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

Alternativamente, você pode atualizar um perfil de máquina usando o Studio.

3. Execute `Set-ProvVMUpdateTimeWindow` para atualizar as VMs de catálogo existentes. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. Após reiniciar as VMs, você pode ver a criptografia de disco atualizada nos discos da VM no portal do Azure.
5. Execute `Set-ProvScheme` para desativar a criptografia de disco antes de adicionar novas VMs de catálogo.

> **Nota:**
>
> Esta etapa é necessária porque você está atualizando um catálogo de ponto de extremidade privado. Se você não realizar esta etapa, receberá erros ao tentar adicionar novas VMs ao catálogo.
>
> Por exemplo:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

6. Adicione novas VMs ao catálogo.

ATUALIZAR VMS DE CATÁLOGO INDIVIDUAIS

As etapas detalhadas para atualizar VMs de catálogo individuais são as seguintes:

1. Crie um catálogo sem criptografia de disco através de `ProxyHypervisorTrafficThroughConnector`. Para obter mais informações sobre

`ProxyHypervisorTrafficThroughConnector`, consulte Criar um ambiente seguro para tráfego gerenciado pelo Azure.

2. Execute `Set-ProvVM` para atualizar a VM do catálogo com `DiskEncryptionSetId`.

> **Nota:**
>
> O `DiskEcryptionSetId` pode ser configurado por meio de `CustomProperties` ou `MachineProfile`.

Exemplo ao usar `CustomProperties`:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-CustomProperties $customProperties
```

Exemplo ao usar MachineProfile:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

3. Execute `Set-ProvVMUpdateTimeWindow` para atualizar as VMs do catálogo existente. Por exemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01 -StartsNow -DurationInMinutes -1
```

4. Depois de reiniciar as VMs, você pode ver a criptografia de disco atualizada nos discos das VMs no portal do Azure.
5. Adicione novas VMs ao catálogo.

Usar disco temporário como disco WBC para catálogos existentes

Você pode usar o disco temporário do Azure como disco de cache de write-back (WBC) para catálogos de máquinas MCS existentes. Use o comando PowerShell `Set-ProvScheme` para atualizar catálogos e VMs existentes.

Pré-requisitos

O catálogo existente deve satisfazer as seguintes condições:

> **Nota:**
>
> Se o catálogo existente não atender aos requisitos a seguir, o disco WBC não será colocado dentro do disco temporário.

- MCSIO está habilitado: As propriedades personalizadas `WriteBackCacheMemorySize`, `WriteBackCacheDiskSize` e `UseWriteBackCache` estão habilitadas.
- O disco do SO efêmero não está habilitado.
- WBC não é persistente: `PersistWBC` é `false`.
- `UseTempDiskForWBC` é nulo ou falso.
- O tamanho do disco temporário deve ser maior que o tamanho total de (tamanho do disco de cache de write-back + espaço reservado para arquivo de paginação + 1 GB de espaço de buffer).

> **Importante:**
>
> Não é permitido alterar uma oferta de serviço de uma com disco temporário para uma sem, ou vice-versa.

Atualizar catálogos existentes

Para atualizar um catálogo existente, execute os seguintes comandos:

1. Execute `Set-ProvScheme` no catálogo existente para atualizar o `UseTempDiskForWBC` para `true`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName name -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Standard_LRS`"/><Property
xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"ManagedDisksPreview`"
Value=`"False`"/><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"False`"/><Property
xsi:type=`"StringProperty`" Name=`"UseTempDiskForWBC`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"False`"/></CustomProperties>"
```

2. Adicione novas máquinas ao catálogo e ligue-as. As novas VMs têm um disco WBC dentro do disco temporário.

Recuperar informações para VMs do Azure, snapshots, disco do SO e definição de imagem da galeria

Você pode exibir informações para uma VM do Azure, incluindo disco e tipo de SO, snapshot e definição de imagem da galeria. Essas informações são exibidas para recursos na imagem mestre quando um catálogo de máquinas é atribuído. Use essa funcionalidade para visualizar e selecionar uma imagem Linux ou Windows. Uma propriedade do PowerShell, `TemplateIsWindowsTemplate`, foi adicionada ao parâmetro `AdditionDatafield`. Este campo contém informações específicas do Azure: tipo de VM, disco do SO, informações da imagem da galeria e informações do tipo de SO. Definir `TemplateIsWindowsTemplate` como **True** indica que o tipo de SO é Windows e definir `TemplateIsWindowsTemplate` como **False** indica que o tipo de SO é Linux.

> **Dica:**

> As informações exibidas pela propriedade PowerShell `TemplateIsWindowsTemplate` são derivadas da API do Azure. Às vezes, este campo pode estar vazio. Por exemplo, um snapshot de um disco de dados não contém o campo `TemplateIsWindowsTemplate` porque o tipo de SO não pode ser recuperado de um snapshot.

Por exemplo, defina o parâmetro `AdditionData` da VM do Azure como **True** para o tipo de SO Windows usando o PowerShell:

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

Recuperar informações de nome de região para VMs do Azure, discos gerenciados, snapshots, VHD do Azure e modelos ARM

Você pode exibir informações de nome de região para uma VM do Azure, discos gerenciados, snapshots, VHD do Azure e modelos ARM. Essas informações são exibidas para os recursos na imagem mestre quando um catálogo de máquinas é atribuído. Uma propriedade do PowerShell chamada `RegionName` exibe as informações do nome da região quando você executa o comando do PowerShell com o parâmetro `AdditionalData`.

Por exemplo, use o seguinte comando PowerShell para obter informações de uma VM no Azure.

```
PS C:\Windows\system32> (get-item XDHyp:
\HostingUnits\myAzureNetwork\image.folder\hu-dev-testing-
rg.resourcegroup\hu-dev-tsvda.vm).AdditionalData

Key Value
```

```
HardDiskSizeGB 127

ResourceGroupName HU-DEV-TESTING-RG

RegionName East US

TemplateIsWindowsTemplate True

LicenseType

ServiceOfferingDescription Standard_B2ms

ServiceOfferingMemory 8192

ServiceOfferingCores 2

SupportedMachineGenerations Gen1,Gen2

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SecurityType

SecureBootEnabled

VTpmEnabled
```

Clonar um catálogo MCS

Divida um catálogo MCS persistente e não persistente existente em vários catálogos. Ao criar um clone do esquema de provisionamento original, você pode aplicar diferentes políticas e configurações de nível de catálogo a subconjuntos específicos de VMs. Essa funcionalidade é particularmente útil quando diferentes funções dentro de uma organização, como Finanças ou Executivos, exigem configurações de recursos diferentes (por exemplo, limites de backup) em comparação com os usuários padrão.

Exemplo de uso

Um administrador gerencia um grande catálogo de VMs. A equipe Executiva exige um número maior de backups do que o permitido pela política padrão. O administrador usa o comando `Copy-ProvScheme` para clonar o esquema de provisionamento de catálogo existente em um novo catálogo. Isso permite que o administrador aplique uma política de backup dedicada ao novo catálogo Executivo, mantendo as configurações originais para o restante da organização.

Aplicabilidade

- Ambientes Azure
- Catálogos MCS persistentes e não persistentes
- Catálogos Citrix Provisioning provisionados por MCS

Limitações

- **Esquema de provisionamento:** Somente a versão mais recente do esquema de provisionamento é copiada.
- **Agendamentos de backup**: O agendamento de backup não é copiado para o novo catálogo; o novo catálogo deve ter seu próprio agendamento de backup configurado.
- **Pools de identidade**: Objetos relacionados à identidade não são clonados e permanecem compartilhados usando o mesmo `ADAccountIdentityPool`.
- **Grupos de entrega**: As operações de grupo de entrega e as atribuições de usuário não são alteradas ou associadas durante o processo de clonagem.

Considerações importantes

- **Grupos de Recursos (TargetLocation)**:
  - Se você não fornecer um `TargetLocation` (Azure Resource Group):
    - Para um grupo de recursos gerenciado pela Citrix, um novo grupo de recursos gerenciado pela Citrix é criado.
    - Para um grupo de recursos BYO (Bring Your Own), os novos recursos do esquema de provisionamento são criados no mesmo grupo de recursos.
  - Se você fornecer um `TargetLocation`:
    - Os recursos são criados no grupo de recursos fornecido.
    - O grupo de recursos especificado já deve existir no Azure.
- **Instantâneo do Disco Base**: Uma cópia do instantâneo do disco base é sempre feita, independentemente da configuração do grupo de recursos.

Pré-requisitos

- Um esquema de provisionamento existente (catálogo de origem) deve estar disponível.
- Se for especificada uma localização de destino, o Grupo de Recursos do Azure de destino deve existir.

Configurar usando PowerShell

1. Abra uma janela do PowerShell.
2. Execute o `Copy-ProvScheme` comando usando os parâmetros necessários: `SourceProvisioningSchemeName` (ou `SourceProvisioningSchemeUid`) e `TargetProvisioningSchemeName`.

   Exemplo 1: Copiar um esquema de provisionamento por nome.

   Este exemplo copia o esquema chamado "Backup" para um novo esquema chamado "TestCopy".

   ```
   Copy-ProvScheme -SourceProvisioningSchemeName Backup
   -TargetProvisioningSchemeName TestCopy
   ```

   Exemplo 2: Copiar um esquema de provisionamento por Uid para um Grupo de Recursos específico

   Este exemplo copia um esquema usando seu Uid e especifica um grupo de recursos de destino chamado "TestRg".

   ```
   Copy-ProvScheme -SourceProvisioningSchemeUid 771e205d-1ee5-4ad2-b044-
   ecf3d7f24ec7 -TargetProvisioningSchemeName TestCopy -TargetLocation
   TestRg
   ```

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos na plataforma Azure. As tags na tabela são representadas como "chave":"valor".

NOME DO RECURSO	TAG
Disco de ID	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
Imagem	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"

NOME DO RECURSO	TAG
NIC	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
Disco do SO	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
VM de preparação	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
Instantâneo publicado	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
Grupo de recursos	"CitrixResource" : "Internal"
	CitrixSchemaVersion: 2.0
	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Conta de armazenamento	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
VM no catálogo	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"
Disco WBC	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "Internal"

> **Nota:**

> Uma VM não fica visível no inventário do Citrix se uma tag **CitrixResource** for adicionada para identificá-la como um recurso criado pelo MCS. Você pode remover ou renomear a tag para torná-la visível.

Remover tags

Ao criar um catálogo ou uma VM, as tags são criadas nos seguintes recursos:

- Grupo de recursos
- Máquina virtual
- Disco do SO
- Disco de identidade
- Interface de rede
- Conta de armazenamento

Você pode remover VMs e catálogos de máquinas do banco de dados Citrix e remover tags. Você pode usar:

- `Remove-ProvVM` com o parâmetro `ForgetVM` para remover VMs e tags de uma única VM ou de uma lista de VMs de um catálogo de máquinas.
- `Remove-ProvScheme` com o parâmetro `ForgetVM` para remover um catálogo de máquinas do banco de dados Citrix e tags de um catálogo de máquinas inteiro.

Este recurso é aplicável apenas a VMs persistentes.

Para fazer isso:

1. Abra uma janela do **PowerShell**.
2. Execute **asnp citrix*** para carregar os módulos PowerShell específicos da Citrix.
3. Execute `Remove-ProvVM` para excluir VMs do banco de dados Citrix e tags de VMs. Por exemplo:

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName “vmname” -ForgetVM
```

4. Execute `Remove-ProvScheme` para excluir o catálogo de máquinas do banco de dados Citrix e tags dos catálogos de máquinas. Por exemplo:

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName”
-ForgetVM
```

> **Nota:**
>
> Depois de usar o parâmetro `ForgetVM` em `Remove-ProvScheme`, o MCS exclui todos os instantâneos, incluindo o instantâneo do disco base, se o esquema de provisionamento estiver presente em um grupo de recursos próprio (BYORG) ou em um grupo de recursos gerenciado pela Citrix.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o Microsoft Azure
- Criar catálogos de máquinas
- Criar um catálogo do Microsoft Azure
- Gerenciar catálogos de máquinas

Gerenciar um catálogo do Microsoft SCVMM

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de virtualização do Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Antes de gerenciar um catálogo VMM, você precisa concluir a criação de um catálogo VMM. Consulte Criar um catálogo do Microsoft System Center Virtual Machine Manager.

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos na plataforma SCVMM. As tags na tabela são representadas como "chave":"valor".

NOME DO RECURSO	TAG
VM de preparação	String da tag: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	Entrada de propriedade personalizada: "XdConfig:"XdProvisioned=True"
VM no catálogo	String da tag: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	Entrada de propriedade personalizada: "XdConfig:"XdProvisioned=True"

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o Microsoft System Center Virtual Machine Manager
- Criar catálogos de máquinas
- Criar um catálogo do Microsoft System Center Virtual Machine Manager
- Gerenciar catálogos de máquinas

Gerenciar um catálogo Nutanix

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes Nutanix AHV Prism Central.

> **Nota:**

> Antes de gerenciar um catálogo de máquinas no Nutanix AHV Prism Central, você precisa concluir a criação de um catálogo de máquinas no Nutanix AHV Prism Central. Consulte Criar um catálogo Nutanix.

> Você pode gerenciar um catálogo de máquinas no Nutanix AHV Prism Central usando:

- Studio
- PowerShell

Usar o Studio

A seguir estão as opções para gerenciar um catálogo de máquinas no Nutanix AHV Prism Central usando o Studio:

OPÇÃO	DESCRIÇÃO
Adicionar Máquinas	Crie e adicione VMs ao catálogo de máquinas.
Excluir Catálogo de Máquinas	Exclua um catálogo de máquinas. Você pode optar por excluir VMs ao mesmo tempo ou deixar as VMs persistentes intactas.
Alterar Imagem Mestra	Altere a imagem mestra usada como modelo para todas as VMs no catálogo.
Adicionar ou alterar Perfil de Máquina	Altere a versão do modelo do perfil da máquina ou adicione um perfil da máquina a um catálogo existente.
Gerenciar Conjunto de Configurações	Vincule um catálogo a um conjunto de configurações do Workspace Environment Management™ ou mude para uma configuração diferente.
Editar Catálogo de Máquinas	Modifique as configurações do catálogo, como NICs e Máquinas Virtuais.
Visualizar Máquinas	Vá para o nó **Pesquisar** para ver todas as VMs que pertencem ao catálogo.
Renomear Catálogo de Máquinas	Altere o nome do catálogo.
Atualizar VDAs	Atualize os VDAs por catálogo. Este recurso se aplica apenas a máquinas persistentes estáticas.
Alterar Nível Funcional	Selecione o nível funcional mínimo para o catálogo. Definir um nível funcional torna todos os recursos disponíveis.
Testar Catálogo de Máquinas	Verifique se o catálogo tem erros ou avisos.

OPÇÃO	DESCRIÇÃO
Gerenciar Tags	Crie, edite e exclua tags. Selecione as tags para aplicar ao catálogo.
Mover Catálogo de Máquinas	Mova o catálogo para outra pasta.

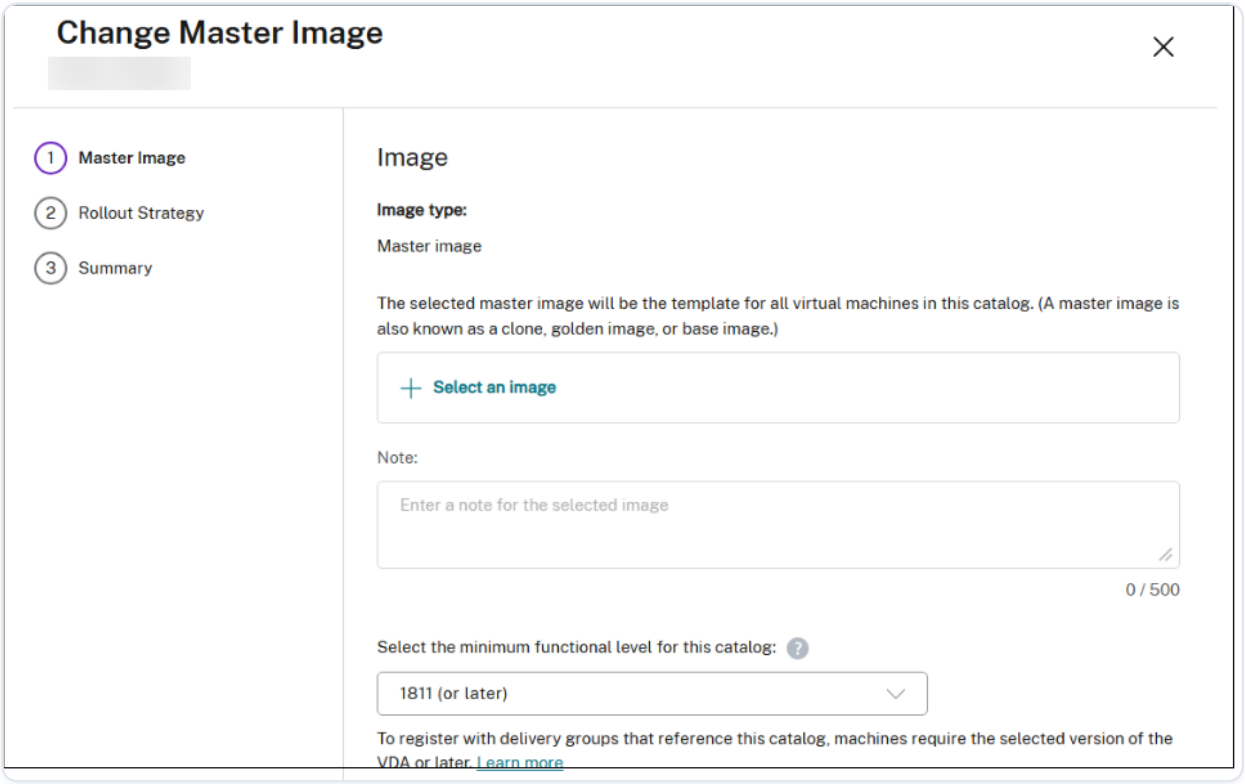
Nota:

Atualmente, a opção **Clonar** não está disponível.

Alterar imagem mestre

Para alterar a imagem mestre de um catálogo, siga estas etapas:

1. Na página **Catálogos de Máquinas**, clique com o botão direito do mouse no catálogo de máquinas que você deseja atualizar e selecione **Alterar Imagem Mestre**.
2. Na página **Alterar Imagem Mestre**, clique em **Selecionar uma imagem**.



3. Na página **Selecionar uma imagem**, expanda um modelo e selecione uma versão de modelo para usar como imagem mestre. Você pode filtrar modelos de máquina por nome.

4. Na página **Estratégia de Implantação**, escolha quando você deseja que a atualização seja aplicada.

Nota:

- Para um catálogo não persistente provisionado por MCS com o plug-in de conexão do host Nutanix AHV Prism Central, a atualização da imagem mestre para alternar a configuração de inicialização entre Legacy e UEFI impede que as VMs existentes iniciem na próxima inicialização.
- Ao atualizar a imagem mestre, apenas o disco do SO é atualizado. As propriedades de hardware permanecem inalteradas. Para atualizar as propriedades de hardware, consulte Adicionar ou alterar o perfil da máquina, Alterar NICs e Alterar a configuração das VMs.

Adicionar ou alterar o perfil da máquina

Para adicionar ou alterar um perfil de máquina para um catálogo, siga estas etapas:

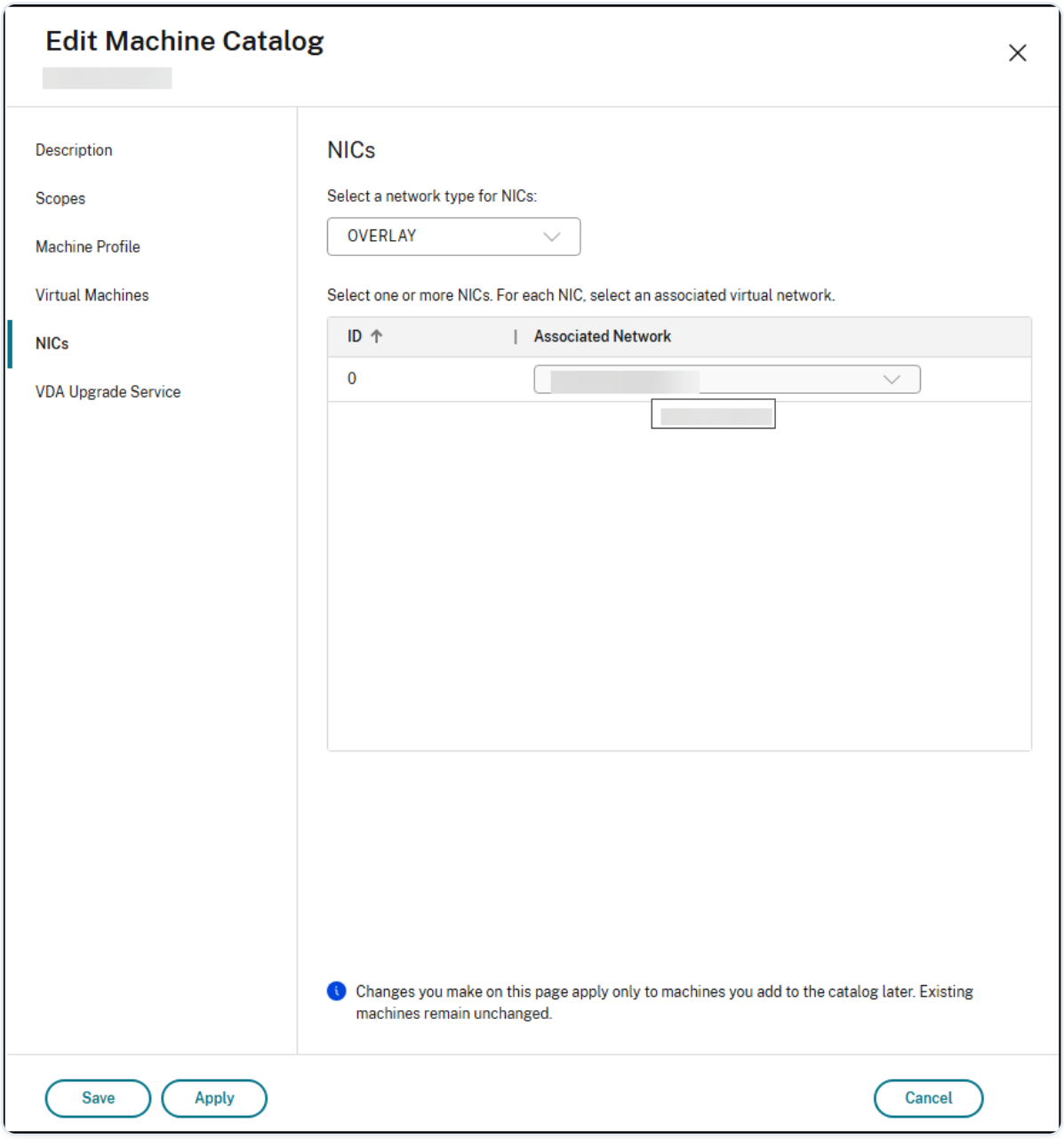
1. Na página **Catálogos de Máquinas**, clique com o botão direito do mouse no catálogo de máquinas que você deseja modificar e selecione **Editar Catálogo de Máquinas**.
2. Na página **Perfil da Máquina**,
   - Se o catálogo de máquinas já tiver um perfil de máquina, clique no ícone de lápis para selecionar uma versão diferente do modelo de perfil de máquina. Você pode filtrar pelo nome do modelo. Confirme as configurações do perfil da máquina.
   - Se o catálogo de máquinas não tiver um perfil de máquina, selecione Usar um perfil de máquina e selecione um perfil de máquina. Confirme as configurações do perfil da máquina.
3. A página **Máquinas Virtuais** deve refletir a configuração atualizada de acordo com a versão do modelo de perfil de máquina selecionada.

Alterar NICs

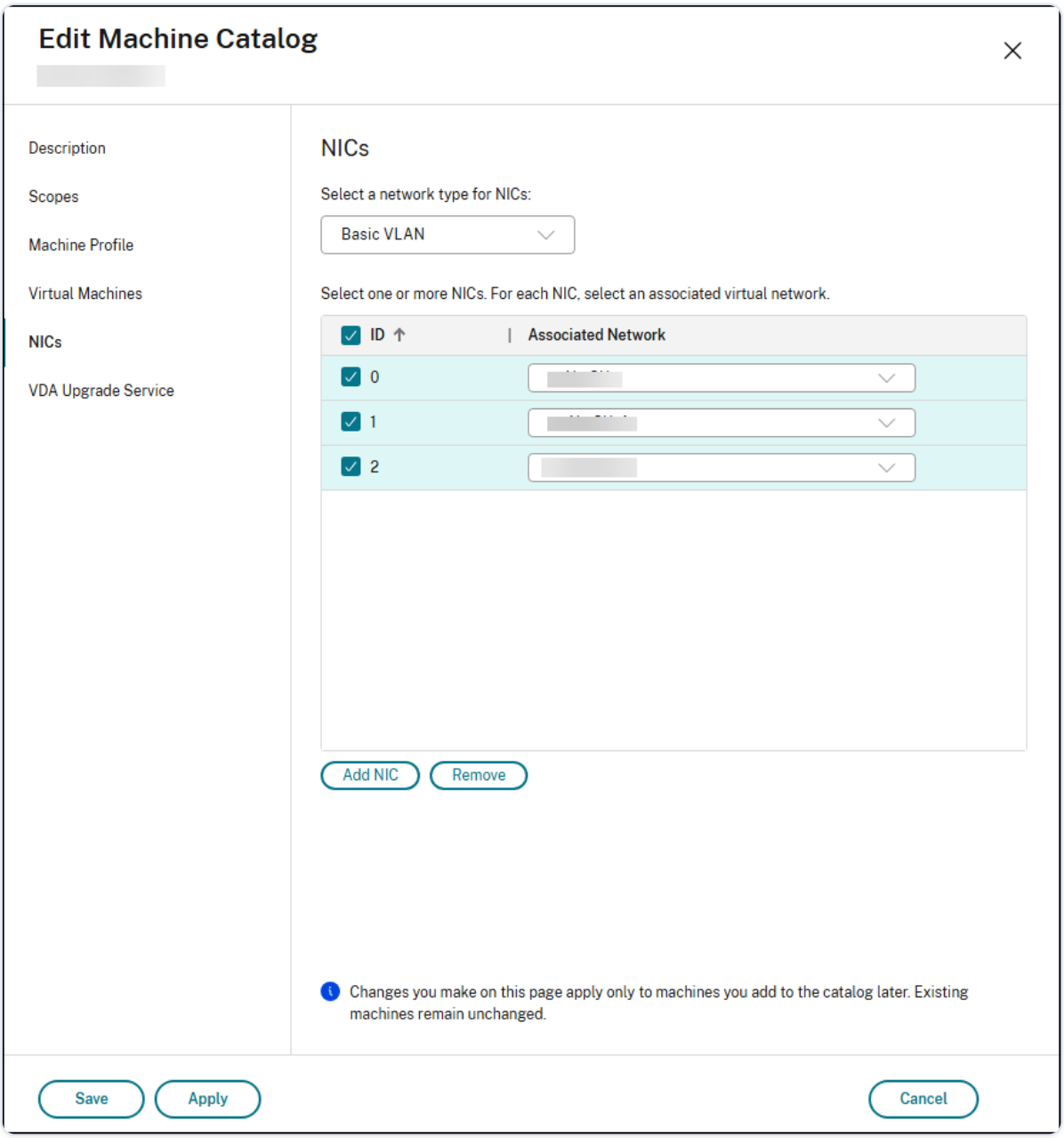
Para alterar as NICs de um catálogo, siga estas etapas:

1. Na página **Catálogos de Máquinas**, clique com o botão direito do mouse no catálogo de máquinas que você deseja modificar e selecione **Editar Catálogo de Máquinas**.
2. Na página **NICs**:

- Selecione um tipo de **NIC**.
- Se o catálogo selecionado foi criado com um perfil de máquina, o número da NIC é consistente com o número da NIC do perfil da máquina e não pode ser alterado. Selecione uma rede virtual associada para cada NIC.



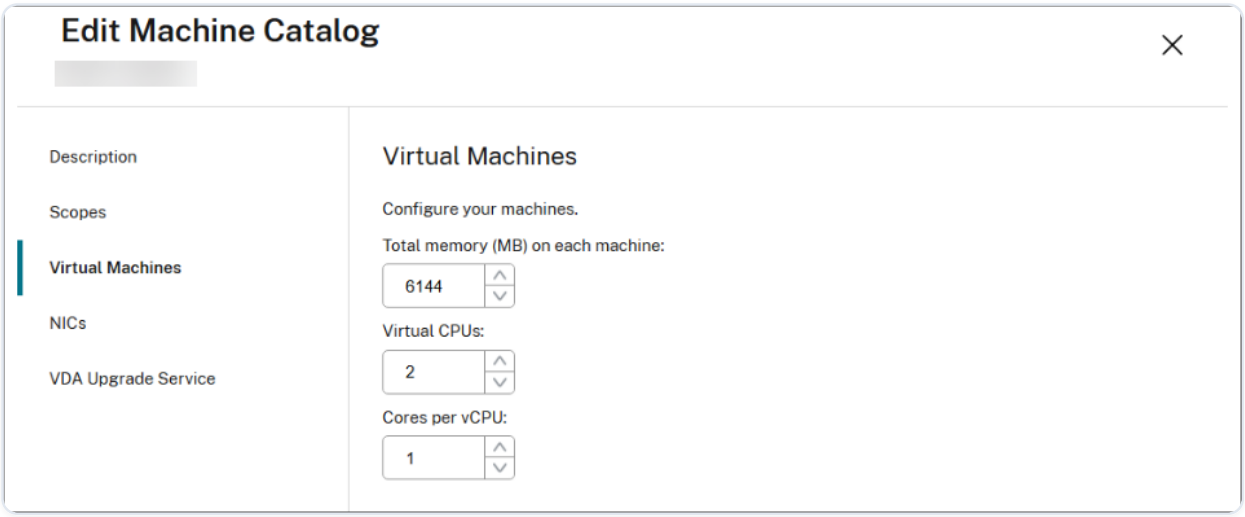
- Se o catálogo selecionado foi criado sem perfil de máquina, clique em **Adicionar NIC** para aumentar a contagem de NICs ou clique em **Remover** para excluir as NICs selecionadas. Selecione ou desmarque as caixas para selecionar as NICs e escolha uma rede virtual associada para cada NIC.



Alterar a configuração das VMs

Para alterar a configuração das VMs, incluindo Memória, contagem de CPU e Cores por vCPU, siga estas etapas:

1. Na página **Catálogos de Máquinas**, clique com o botão direito do mouse no catálogo de máquinas que deseja modificar e selecione **Editar Catálogo de Máquinas**.
2. Na página **Máquinas Virtuais**, use a seta para cima ou para baixo, ou insira valores diretamente para ajustar a Memória, a contagem de CPU e os Cores por vCPU para as VMs.



Usar PowerShell

Alterar imagem mestre

Os parâmetros necessários são:

- `ProvisioningSchemeName`: Nome do esquema de provisionamento a ser editado.
- `MasterImage`: Caminho literal para a nova imagem mestre.

Execute o seguinte comando. Por exemplo:

```
Set-ProvSchemeMetadata  -Name "ImageManagementPrep_DoImagePreparation"
-ProvisioningSchemeName "<ProvisioningSchemeName>" -Value "True"



Publish-ProvMasterVMImage  -MasterImageVM "<Literal path to the new master
image- template version> -ProvisioningSchemeName
"<ProvisioningSchemeName>" -RunAsynchronously
```

> **Nota:**
>
> Ao atualizar a imagem mestre, apenas o disco do SO é atualizado. As propriedades de hardware permanecem inalteradas. Para atualizar as propriedades de hardware, consulte Adicionar ou alterar o perfil da máquina, Alterar NICs e Alterar NIC e configuração da VM.

Adicionar ou alterar perfil da máquina

Use o comando `Set-ProvScheme`:

- Para atualizar um catálogo com um novo perfil de máquina, ou
- Para atualizar um catálogo existente que não possui um perfil de máquina para começar a usar o perfil da máquina como a fonte da especificação de hardware.

Nota:

Isso não atualiza a especificação de hardware das VMs existentes no catálogo. Apenas as novas VMs adicionadas ao catálogo terão a especificação de hardware do perfil de máquina fornecido.

Para alterar o perfil da máquina ou converter um catálogo existente para começar a usar o perfil da máquina:

```
Set-ProvScheme -ProvisioningSchemeName <ProvScheme Name> `

               -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion"

               -NetworkMapping @{"0"="XDHyp:\HostingUnits\<Hosting unit
name>\Clusters.folder\<Cluster Name>.cluster\<Network name>.network"}
```

O perfil da máquina deve ter pelo menos uma NIC, e o número de NICs no perfil da máquina deve corresponder aos mapeamentos de sub-rede em NetworkMapping

O número total de NICs para a versão do modelo pode ser obtido do `AdditionalData` de seu item de inventário usando o seguinte:

```
$tv = Get-Item -Path "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion"

$tv.AdditionalData.TotalNics
```

Para alterar o perfil da máquina com especificação de hardware substituída:

Certas configurações podem ser configuradas usando parâmetros de linha de comando específicos. Esses parâmetros de linha de comando, como `VMCpuCount` e `VMMemoryMB`, e

`CPUCores` no `CustomProperties`, têm precedência sobre os valores na versão do modelo de Perfil da Máquina.

```
$customProperties = @"

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

        <StringProperty Name="ClusterId"
Value="00062c63-1fb0-58c9-4fc8-5c2573352378" />

        <StringProperty Name="CPUCores" Value="2" />

    </CustomProperties>

"@



Set-ProvScheme -ProvisioningSchemeName <ProvScheme Name> `

               -MachineProfile "XDHyp:\HostingUnits\<Hosting Unit
Name>\Templates.folder\<Template Name>.template\<Template Version
Name>.templateversion" `

               -CustomProperties $customProperties `

               -VMCpuCount 4 `

               -VMMemoryMB 4096
```

Alterar NIC e configuração da VM

Os parâmetros necessários são:

- `ProvisioningSchemeName`: Nome do esquema de provisionamento a ser editado.
- `NetworkMapping`: Mapeamento de rede atualizado.

Execute o seguinte comando. Por exemplo:

```
Set-ProvScheme  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`"
Name=`"ClusterId`" Value=`"000xxxx-1fb0-xxxxx-4fc8-5c257335xxxx`" /
><Property xsi:type=`"StringProperty`" Name=`"CPUCores`" Value=`"1`" /></
CustomProperties>"  -NetworkMapping @{"6"="XDHyp:\HostingUnits\<Hosting
Unit Name>\Clusters.folder\<Cluster Name>\<Network name>.network"}
-ProvisioningSchemeName "<ProvisioningSchemeName>" -VMCpuCount 4
```

Redefinir disco do SO para VMs persistentes

Redefinir o disco do SO em VMs persistentes, especialmente aquelas com vTPM habilitado, pode quebrar aplicativos que dependem de chaves vTPM e BitLocker, potencialmente impedindo a inicialização. Portanto, este recurso permite:

- Redefinir o disco do SO para VMs persistentes e preservar as configurações de hardware da VM.
- Gerenciar VMs habilitadas para vTPM para evitar quebrar a dependência de vTPM durante trocas de disco.

Você pode redefinir o disco do SO para VMs persistentes usando o comando PowerShell `Reset-ProvVMDisk`.

- Para VMs habilitadas para vTPM: Uma nova VM é criada a partir de um ponto de recuperação usando as informações de hardware originais, preservando as chaves vTPM.
- Para VMs sem vTPM: O disco do SO é substituído.

Para exemplos, consulte Redefinir disco do SO.

Migrar catálogos de máquinas para a conexão de host Nutanix AHV Prism Central gerenciada pela Citrix

Migre seus catálogos de máquinas Citrix e suas VMs associadas das conexões de host existentes do Nutanix AHV (para Prism Element) e Nutanix AHV PC (para NC2 no Azure) para a conexão de host Nutanix AHV Prism Central gerenciada pela Citrix. Para a migração, use comandos PowerShell, que também incluem opções de reversão rápida em caso de problemas e comandos para limpar os recursos de origem após a migração.

Benefícios

- **Interrupção minimizada**: Você faz a transição suavemente para o plug-in Nutanix AHV Prism Central. Isso tem um impacto mínimo em suas implantações existentes.

- **Caminho de atualização contínuo**: Ele fornece um caminho claro e suportado para você atualizar sua infraestrutura e aproveitar a nova interface de gerenciamento.
- **Integridade e segurança dos dados**: As opções de reversão garantem que você reverta o ambiente para o seu estado original em caso de problemas imprevistos. Isso reduz o risco.
- **Eficiência de recursos**: Você limpa os recursos de origem após a migração bem-sucedida. Isso otimiza o armazenamento e a sobrecarga de gerenciamento.
- **Flexibilidade**: Ele suporta a migração para catálogos provisionados tanto por MCS quanto por tecnologias de terceiros. Isso oferece uma aplicabilidade mais ampla.

Aplicabilidade

Este recurso é aplicável a catálogos de máquinas sob conexões de host Nutanix AHV (para Prism Element) e Nutanix AHV PC (para NC2 no Azure):

- Catálogos de máquinas gerenciados por MCS, incluindo tipos persistentes e não persistentes.
- Catálogos de máquinas somente gerenciados por energia que contêm VMs provisionadas por tecnologias de terceiros.

Requisitos do Sistema

- **Versão do AOS do Nutanix AHV Prism Element (PE)**: Você precisa de um mínimo de 6.8.
- **Versão do Nutanix Prism Central (PC)**: Você precisa de um mínimo de 2024.3.

> **Nota:**
>
> O Nutanix Prism Central 7.3 requer o AOS 7.3 devido a um problema conhecido do Nutanix.

Limitações

- **Catálogos PVS não são suportados**: Este recurso **NÃO** suporta catálogos de máquinas criados usando o Assistente de Configuração do Xendesktop do **Citrix Provisioning Services** (PVS).
- **Restrições de reversão**:
  - Permita a reversão de um catálogo migrado apenas se você **NÃO** tiver modificado o catálogo após a migração inicial.
  - Ao executar a operação "**Limpar Recursos de Origem**", ela limpa o estado da migração. Isso impede qualquer reversão subsequente.

- **Sem remigração**: Um catálogo de máquinas que você já migrou não é suportado para remigração.
- **VMs de conexão multi-host**: A migração de catálogos de máquinas somente gerenciados por energia que contêm VMs importadas de várias conexões de host não é suportada.

Considerações Importantes

- **Gerenciamento de cluster Nutanix**: Os clusters Nutanix AHV de hospedagem devem ser registrados em um Nutanix Prism Central. .
- **Criação de modelo de imagem mestre**: Para catálogos de máquinas MCS, o comando de migração oferece uma opção para gerar uma versão de modelo de VM no Prism Central a partir do snapshot original da imagem mestre do catálogo de máquinas. Esta versão de modelo de VM pode ser usada posteriormente como a imagem mestre MCS de catálogos de máquinas sob conexão de host do Prism Central. Por padrão, esta opção não está habilitada.
- **Pré-condições de reversão**:

  Para que uma reversão bem-sucedida seja possível, o ambiente de origem original — incluindo a conexão do host, discos base — deve permanecer inalterado. Você também deve evitar fazer quaisquer alterações de configuração no catálogo de máquinas migrado e adicionar/remover VMs até que a migração seja confirmada como bem-sucedida. Após essa confirmação, você pode executar a operação final Limpar Recursos de Origem, mas esteja ciente de que este é um passo irreversível que tornará a reversão impossível.

Permissões necessárias para migração e reversão

Para migrar catálogos ou reverter, você precisa das seguintes permissões:

Administrador do Prism Element:

- Criar Máquina Virtual

Administrador do Prism Central:

- Criar Modelos de VM
- Excluir Modelos de VM
- Excluir Ponto de Recuperação de VM
- Excluir Máquina virtual

Para a lista completa de permissões específicas necessárias para a conexão de host do Nutanix AHV Prism Central gerenciada pelo Citrix, consulte Permissões necessárias.

Como migrar

Você gerencia esse recurso por meio de cmdlets PowerShell dedicados. O fluxo de trabalho geral envolve três operações principais: Migração, Reversão e Limpeza de recursos de origem.

Migrar um catálogo de máquinas

- Esta operação move um catálogo de máquinas e suas VMs associadas de uma conexão de host Nutanix AHV ou Nutanix AHV PC de origem para uma conexão de host Nutanix AHV Prism Central gerenciada pelo Citrix de destino.
- Para catálogos provisionados por MCS, este processo cria novos discos base na conexão de destino.
- Opcionalmente, você pode optar por criar um equivalente de VM mestre (versão de modelo de VM) na conexão de destino a partir do snapshot da imagem mestre original.

1. **Criar uma nova conexão de host do Nutanix AHV Prism Central**: Antes de migrar, registre o cluster Nutanix AHV de hospedagem em um Nutanix Prism Central e estabeleça uma nova conexão de host do Nutanix AHV Prism Central que aponte para a instância de destino do Nutanix Prism Central. Essa conexão serve como destino para seus catálogos migrados. Para obter detalhes, consulte Conexão de host do Nutanix AHV Prism Central.
2. **Migrar um catálogo de máquinas existente**: Para catálogos de máquinas existentes, use o cmdlet PowerShell `Switch-ProvCatalog` para iniciar a migração para a conexão de host do Nutanix AHV Prism Central gerenciada pelo Citrix.

   ```
   c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID>
   -DestinationHypervisorConnectionName "DestinationConnection"
   -DestinationHostingUnitName "DestinationUnit"
   -CreateMasterImageAtDestination
   ```

   - Substitua `<Catalog_UID>` pelo identificador exclusivo do catálogo de máquinas que você deseja migrar. Use o seguinte cmdlet PowerShell para localizar o `BrokerCatalogUid` pelo nome do catálogo `Get-BrokerCatalog -Name <Catalog Name>`.
   - `DestinationConnection` é o nome da nova **conexão de host do Nutanix AHV Prism Central** criada na Etapa 1.
   - `DestinationUnit` é o nome que você dá à unidade de hospedagem dentro do `DestinationConnection` onde o catálogo de máquinas residirá.
   - O parâmetro `-CreateMasterImageAtDestination` é opcional. Ele cria uma versão de modelo de VM de imagem mestre no Prism Central de destino.

3. **Verificar a conclusão da migração**: Após executar o cmdlet de migração, monitore o status da tarefa na janela do PowerShell para garantir que ela seja concluída com êxito. Quando a migração for concluída, o catálogo será movido para a conexão de host de destino criada na etapa 1. Você deve ver um status de concluído com o tipo de tarefa SwitchProvCatalog. A seguir estão as etapas recomendadas para verificar a conclusão da migração:

    - Verifique o status do catálogo no Studio.
    - Verifique se as VMs dentro do catálogo estão agora associadas à nova conexão de hipervisor de destino.
    - Verifique se as VMs dentro do catálogo estão mostrando o estado de energia correto.
    - Teste a funcionalidade do catálogo de máquinas migrado adicionando ou removendo máquinas ou emitindo operações de energia, garantindo que o catálogo esteja funcionando corretamente.

Reverter um catálogo migrado

Esta operação reverte um catálogo de máquinas e suas VMs para a conexão de host de origem original. Ela remove quaisquer recursos que você criou durante o processo de migração.

> **Importante:**

> Você só executa a reversão se não tiver modificado o catálogo após a migração e não tiver executado a operação **Limpar Recursos de Origem**. A conexão de origem original permanece inalterada e ainda contém seus discos base.

```
c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID> -Rollback
```

Limpar recursos de origem

Após uma migração bem-sucedida, esta operação remove os recursos de origem, por exemplo, discos base, da conexão do hipervisor original.

> **Importante:**

> Ao executar este comando, ele limpa o estado da migração. Isso torna as reversões subsequentes impossíveis.

```
c:\PS>Switch-ProvCatalog -BrokerCatalogUid <Catalog_UID>
-CleanupSourceResources
```

Você recebe um prompt de confirmação antes de prosseguir, pois esta ação é irreversível. Confirme o prompt para concluir a limpeza.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com Nutanix
- Conexão com a nuvem Nutanix e soluções de parceiros
- Criar catálogos de máquinas
- Criar um catálogo Nutanix
- Gerenciar catálogos de máquinas

Gerenciar um catálogo VMware

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos para ambientes de virtualização VMware.

> **Nota:**
>
> Antes de gerenciar um catálogo VMware, você precisa concluir a criação de um catálogo VMware. Consulte Criar um catálogo VMware.

Atualizar VMs provisionadas para o estado atual do esquema de provisionamento

O comando `Set-ProvScheme` altera o esquema de provisionamento. No entanto, ele não afeta as VMs existentes. Usando o comando PowerShell `Set-ProvVMUpdateTimeWindow`, você pode aplicar o esquema de provisionamento atual a uma VM ou conjunto de VMs persistentes ou não persistentes existentes. Esse recurso é aplicável a catálogos de máquinas baseados em perfil de máquina e não baseados em perfil de máquina.

Você pode atualizar o seguinte:

- VMCpuCount: Propriedade do esquema de provisionamento
- VMMemoryMB: Propriedade do esquema de provisionamento

- ID da Pasta: Propriedade personalizada
- Mapeamento de sub-rede: Propriedade do esquema de provisionamento
- Versão de hardware da VM: Somente para catálogo de máquinas baseado em perfil de máquina
- Perfil de máquina: Somente para catálogo de máquinas baseado em perfil de máquina

Você pode atualizar:

- Uma única VM
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um ID de esquema de provisionamento
- Uma lista de VMs específicas ou todas as VMs existentes associadas a um nome de esquema de provisionamento (nome do catálogo de máquinas)

Antes de atualizar as VMs existentes

1. Verifique a configuração das VMs existentes. Por exemplo:

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. Atualize o esquema de provisionamento. Por exemplo:

```
$customProperties=<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="FolderId"
Value="FOLDER_ID"/></CustomProperties>

$memoryMb=<DOUBLE THE "UPDATE" MACHINE PROFILE>

Set-ProvScheme -ProvisioningSchemeName my-catalog -VMCpuCount 4
-VmMemoryMb $memoryMb -CustomProperties $customerProperties
-NetworkMapping @{"1" = "<A_NETWORK_PATH_FROM_THE_HOSTING_UNIT>"}
-MachineProfile "<PATH_TO_UPDATE_MACHINE_PROFILE>"
```

3. Verifique se a propriedade atual da VM corresponde ao esquema de provisionamento atual e se há alguma ação de atualização pendente na VM. Por exemplo:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

Você também pode encontrar VMs com uma versão específica. Por exemplo:

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

Solicitar atualizações para VMs existentes para aplicar na próxima reinicialização

1. Execute os seguintes comandos para atualizar as VMs existentes e fazer com que as atualizações sejam aplicadas na próxima reinicialização.

   - Para atualizar todas as VMs existentes. Por exemplo:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - Para atualizar uma lista de VMs específicas. Por exemplo:

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
     ```

   - Para atualizar VMs com base na saída de `Get-ProvVM`. Por exemplo:

     ```
     Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
     ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
     -DurationInMinutes -1
     ```

   Nota:

   - O `StartsNow` indica que a hora de início agendada é a hora atual.
   - O `DurationInMinutes` com um número negativo (por exemplo, –1) indica que não há limite superior para a janela de tempo do agendamento.

2. Encontre VMs com uma atualização agendada. Por exemplo:

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. Reinicie as VMs. No próximo ligamento, as alterações de propriedade são aplicadas às VMs existentes. Você pode verificar o status atualizado usando o seguinte comando. Por exemplo:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

Cancelar a atualização da configuração

Você também pode cancelar uma atualização de configuração de uma única VM, várias VMs ou um catálogo inteiro. Para cancelar uma atualização de configuração:

1. Execute `Clear-ProvVMUpdateTimeWindow`. Por exemplo:

   - Para cancelar a atualização de configuração agendada para uma única VM:

     ```
     Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
     -VMName “vm1”
     ```

   - Para cancelar a atualização de configuração agendada para várias VMs:

     ```
     Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
     -VMName "vm1","vm2"
     ```

     > **Nota:**
     >
     > As VMs devem ser do mesmo catálogo.

Atualizar o ID da pasta de um catálogo de máquinas

Você pode atualizar o ID da pasta de um catálogo de máquinas MCS especificando `FolderId` nas propriedades personalizadas do comando `Set-ProvScheme`. As VMs criadas após a atualização do ID da pasta são criadas sob este novo ID de pasta. Se esta propriedade não for especificada em `CustomProperties`, as VMs serão criadas na pasta onde a imagem mestre está localizada.

Execute as seguintes etapas para atualizar o ID da pasta de um catálogo de máquinas.

1. Abra um navegador da Web e insira o URL para o **vSphere Web Client**.
2. Insira as credenciais e clique em **Login**.
3. Crie uma pasta de posicionamento de VM no **vSphere Web Client**.
4. Abra uma janela do PowerShell.
5. Execute **asnp citrix®*** para carregar os módulos PowerShell específicos da Citrix.
6. Especifique o `FolderID` no `CustomProperties` de `Set-ProvScheme`. Neste exemplo, o valor do ID da pasta é `group-v2406`.

```
Set-ProvScheme -ProvisioningSchemeUid
"50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
"<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
Value=""group-v2406"" /></CustomProperties>"
```

7. Adicione uma VM ao catálogo de máquinas usando o Studio.
8. Verifique a nova VM no vSphere Web Client. A nova VM é criada na nova pasta.

Encontrar o ID da pasta usando comandos PowerShell

Use o comando PowerShell `Get-HypConfigurationDataForItem` para encontrar o ID da pasta para uma pasta existente em um Hypervisor VMware.

Crie uma conexão de hospedagem e um grupo de recursos para um Hypervisor VMware. Em seguida, execute as seguintes etapas para encontrar o ID da pasta de uma pasta nesse hypervisor.

1. Determine o caminho `XDHyp` para a raiz da árvore de pastas da VM. Por exemplo:

```
XDHyp:\Connections\VMwareConn\Datacenter.datacenter
```

2. Use `Get-HypConfigurationDataForItem` para recuperar a estrutura da árvore. Por exemplo:

```
Get-HypConfigurationDataForItem -LiteralPath XDHyp:
\Connections\VMwareConn\Datacenter.datacenter
```

3. Execute o seguinte comando para identificar o ID da pasta a partir da saída XML. Neste exemplo, procure o ID da pasta de `ExampleFolder` na saída XML.

```
$result = Get-HypConfigurationDataForItem -LiteralPath XDHyp:
\Connections\VMwareConn\Datacenter.datacenter

$result.VmPlacementFolder
```

Saída XML:

```
<?xml version="1.0" encoding="utf-16"?>

<CtxVmPlacementFolder xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Name>vm</Name>

<Id>group-v4</Id>

<SubFolder>

<CtxVmPlacementFolder>

  <Name>vCLS</Name>

  <Id>group-v75</Id>

  <SubFolder />

</CtxVmPlacementFolder>

<CtxVmPlacementFolder>

  <Name>MyOtherFolder</Name>

  <Id>group-v1110</Id>

  <SubFolder />

</CtxVmPlacementFolder>

<CtxVmPlacementFolder>
```

```
  <Name>ExampleFolder</Name>
  <Id>group-v4658</Id>
  <SubFolder />
</CtxVmPlacementFolder>
</SubFolder>
</CtxVmPlacementFolder>
```

Encontrar o ID da pasta no vSphere

Acesse o MOB em qualquer sistema de servidor ESXi ou vCenter para encontrar o ID da pasta das VMs.

O Managed Object Browser (MOB) é um aplicativo de servidor baseado na web disponível embutido em todos os sistemas de servidor ESX/ESXi e vCenter. Este utilitário vSphere permite visualizar informações detalhadas sobre objetos como VMs, datastores e pools de recursos.

1. Abra um navegador da web e digite `http://x.x.x.x/mob`, onde x.x.x.x é o endereço IP do vCenter Server ou host ESX/ESXi. Por exemplo, `<https://10.60.4.70/mob>`.
2. Na página **Home** do MOB, clique no valor da propriedade **content**.
3. Clique no valor de **rootFolder**.
4. Clique no valor de **childEntity**.
5. Clique no valor de **vmFolder**.
6. Você pode encontrar o ID da pasta no valor de **childEntity**.

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos na plataforma VMware. As tags na tabela são representadas como "key":"value".

NOME DO RECURSO	TAG
VM de preparação	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"

NOME DO RECURSO	TAG
VM no catálogo	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com VMware
- Criar catálogos de máquinas
- Criar um catálogo VMware
- Gerenciar catálogos de máquinas

Gerenciar um catálogo XenServer®

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir cobrem detalhes específicos dos ambientes de virtualização XenServer.

> **Nota:**
>
> Antes de gerenciar um catálogo XenServer, você precisa terminar de criar um catálogo XenServer. Consulte Criar um catálogo XenServer.

Identificar recursos criados pelo MCS

Quando o Machine Creation Services™ (MCS) gera recursos como discos, ele atribui uma tag de ID ProvisioningScheme para melhor utilização desses recursos.

As tags são úteis para os administradores, pois eles podem gerenciar e organizar melhor os recursos. Por exemplo, se recursos, como discos não utilizados, forem marcados com tags, os administradores podem identificar facilmente onde o recurso foi criado, tornando o processo de limpeza eficiente.

A seguir estão as tags que o MCS adiciona aos recursos na plataforma XenServer. As tags na tabela são representadas como "key":"value".

NOME DO RECURSO	TAG
Cópia do disco em cada rede ou armazenamento local (somente no local)	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco de ID	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco do SO	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM de Preparação	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM no catálogo	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco WBC	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Recuperar informações sobre o esquema de provisionamento

Para recuperar informações detalhadas sobre o esquema de provisionamento, você pode executar os seguintes comandos do PowerShell. Substitua `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx` pelo ID real do esquema de provisionamento:

1. Substitua o ID do espaço reservado pelo seu ID real do esquema de provisionamento

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
```

2. Recupere informações detalhadas sobre o esquema de provisionamento:

```
Get-ProvisioningScheme -Id $provisioningSchemeId
```

Recuperar lista de recursos criados pelo MCS

Execute os seguintes comandos para obter uma lista abrangente de recursos criados pelo MCS.

1. Substitua o ID do espaço reservado pelo seu ID real do esquema de provisionamento.

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
```

2. Recupere a lista completa de recursos criados pelo MCS.

```
Get-ProvResource -ProvisioningSchemeUid $provisioningSchemeId |
ConvertTo-JSON -Depth 6
```

Após a execução, você obtém a seguinte saída:

- O nome e o ID do esquema de provisionamento.
- Uma lista de versões de imagem de provisionamento dentro do esquema de provisionamento. Cada entrada inclui:
  - O nome e o ID da imagem.
  - O ID do Disco e o ID do Armazenamento do disco.
- Uma lista de VMs de provisionamento. Cada entrada inclui:
  - O ID do disco do SO e o ID do disco pai do disco do SO.
  - O ID do Armazenamento do disco do SO.
  - O disco de Identidade e seu ID de Armazenamento.

Mais informações

- Criar e gerenciar conexões e recursos
- Conexão com o XenServer
- Criar catálogos de máquinas
- Criar um catálogo do XenServer
- Gerenciar catálogos de máquinas

Gerenciamento de Energia

Com o Citrix DaaS™, você pode gerenciar a energia de VMs provisionadas por MCS em vários hipervisores e serviços de nuvem suportados. A operação de gerenciamento de energia oferece a você:

- Experiência de usuário ideal
- Gerenciamento de custos e economia de energia

As ações de energia disponíveis são:

- Iniciar
- Desligar
- Reiniciar
- Suspender
- Retomar
- Reiniciar forçadamente
- Desligar forçadamente

Nota:

- Para uma VM não persistente, o ciclo de energia (desligar/iniciar e reiniciar) resulta na redefinição do disco do SO.
- As capacidades e comportamentos das ações de energia variam dependendo dos hipervisores ou serviços de nuvem.

O artigo aborda os principais recursos de gerenciamento de energia associados a certos hipervisores suportados.

- Gerenciar energia de VMs Amulet Hotkey CoreStation(/pt-br/citrix-daas/install-configure/power-management/power-manage-amulet-hotkey.html)
- Gerenciar energia de VMs AWS(/pt-br/citrix-daas/install-configure/power-management/power-manage-aws-vms.html)
- Gerenciar energia de VMs Azure(/pt-br/citrix-daas/install-configure/power-management/power-manage-azure-vms.html)

Gerenciar energia de VMs Amulet Hotkey CoreStation

O Citrix DaaS™ permite gerenciar a energia de VMs Amulet Hotkey CoreStation. Use o nó **Pesquisar** no painel de navegação para localizar a máquina que você deseja gerenciar a energia.

As seguintes ações de energia estão disponíveis:

- Iniciar
- Desligar
- Desligamento Forçado

- Reinicialização Forçada
- Reiniciar

> **Nota:**
>
> - As ações de energia Redefinir, Suspender e Retomar não são suportadas.
> - Desligar/Reiniciar: Solicita ao nó que desligue o sistema operacional e o desligue. Isso é equivalente a um breve toque no botão de energia de uma máquina desktop física. A Estação de Trabalho pode não responder à solicitação de desligamento se houver usuários ativos ou programas em execução que interrompam o desligamento ou se as atualizações do sistema operacional precisarem ser instaladas.

Mais informações

- Ambientes de virtualização Amulet Hotkey CoreStation
- Conexão com Amulet Hotkey CoreStation
- Criar um catálogo de máquinas Amulet Hotkey CoreStation

Gerenciar energia de VMs AWS

Para obter informações sobre as permissões necessárias, consulte Sobre as permissões da AWS.

Provisionamento sob demanda da AWS

Com este provisionamento sob demanda, o disco do SO é excluído quando você desliga uma VM não persistente. Depois de ligar a VM, uma nova VM é criada a partir da imagem mestre que possui um disco de SO e um disco de ID. Para determinar se uma VM tem o recurso sob demanda ativado ou não, execute o comando PowerShell `Get-ProvVM`. Se a propriedade `CustomVMData` tiver todos os valores específicos da VM, isso implica que a VM tem o recurso sob demanda ativado.

Hibernação de Instância

O processo de hibernação armazena o estado em memória da instância, juntamente com seus endereços IP privados e elásticos, permitindo que ela retome exatamente de onde parou.

Quando uma instância é instruída a hibernar, ela grava o estado em memória em um arquivo no volume EBS raiz e, em seguida, se desliga. Um volume Amazon EBS é um dispositivo de armazenamento durável, em nível de bloco, que você pode anexar às suas instâncias. Depois de

anexar um volume a uma instância, você pode usá-lo como usaria um disco rígido físico. Criptografe o volume EBS raiz da instância. A criptografia garante a proteção adequada para dados confidenciais quando são copiados da memória para o volume EBS. Para obter informações sobre a criptografia EBS, consulte Criptografia Amazon EBS.

A seguir estão as limitações da hibernação de instância suportada:

- Memória da instância (RAM) de apenas até 150 GB é suportada
- O modo de inicialização UEFI não é suportado
- Os SSDs de uso geral e os SSDs de IOPS provisionadas são suportados apenas como tipos de volume EBS.

Criar VMs com suporte a hibernação

Para criar VMs com suporte a hibernação:

1. Crie uma conexão de host. Consulte Conexão com a AWS.
2. Inicie uma instância com o EBS raiz criptografado e a propriedade **Stop-Hibernate** ativada. Para obter mais informações, consulte:
    - Ciclo de vida da instância
    - Criptografia do Amazon EBS
    - Pré-requisitos de hibernação
    - Habilitar hibernação para uma instância
    - Hibernar sua instância sob demanda ou instância spot
3. Use esta instância como uma imagem mestre para criar uma AMI.
4. Prepare a imagem mestre:
    a. Instale um VDA na imagem mestre. A Citrix recomenda instalar a versão mais recente para permitir o acesso aos recursos mais novos. A falha na instalação de um VDA na imagem mestre faz com que a criação do catálogo falhe. Para obter mais informações sobre como instalar um VDA, consulte Instalar VDAs.
    b. Una a imagem mestre ao domínio do qual os aplicativos e desktops são membros. Certifique-se de que a imagem mestre esteja disponível no host onde as máquinas são criadas.
5. Crie uma AMI a partir dessa instância. Para obter informações sobre como criar uma AMI a partir de uma instância, consulte Criar uma AMI a partir de uma instância do Amazon EC2.

6. Crie um catálogo de máquinas usando o comando `New-ProvScheme`. Defina a propriedade personalizada `AwsCaptureInstanceProperties` como **True**.

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

-CustomProperties "AwsCaptureInstanceProperties,true;"

-HostingUnitName "xxx" -IdentityPoolName $catalog_name
-InitialBatchSizeHint 1

-MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
(vpc-0f1771e45671aedcd).network"}

-ProvisioningSchemeName $catalog_name

-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
"xxx"
```

   Para obter informações sobre como criar um catálogo de máquinas usando comandos PowerShell, consulte `<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>`.

As VMs que podem ser hibernadas são criadas se:

- Você selecionar uma AMI criada a partir de uma imagem mestre que tenha a propriedade **Stop-Hibernate** habilitada.
- A VM mestre estiver unida ao domínio e tiver o VDA instalado.
- Você seleciona o tamanho correto da VM (oferta de serviço) que pode manipular a hibernação.

O comando **New-ProvScheme** falha com uma mensagem de erro apropriada se:

- A VM mestre está habilitada para hibernação, mas a oferta de serviço não é capaz de lidar com a hibernação.
- Se a VM mestre não estiver ingressada no domínio e não tiver nenhum VDA instalado.

Status de hibernação de ofertas de serviço e AMI

Para obter o status de hibernação das ofertas de serviço e AMI (modelos), execute os seguintes comandos:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

Atualizar oferta de serviço de um esquema de provisionamento existente com suporte a hibernação

1. Execute o comando `Set-ProvScheme`. Por exemplo,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <String>
```

O sistema exibe uma mensagem de exceção se a oferta de serviço não for compatível.

Criar catálogo de máquinas com suporte a hibernação

Ao criar catálogos de máquinas, você pode usar um perfil de máquina que suporte hibernação.

1. No assistente de criação de catálogo, siga as instruções até a seleção do perfil da máquina.
2. Na página **Modelo de Máquina**, clique em **Selecionar um perfil de máquina** e selecione um perfil de máquina.
3. Na página **Máquina Virtual**, clique no ícone **Editar** e selecione uma VM.

> **Nota:**
>
> Se o perfil da máquina estiver habilitado para hibernação, o sistema exibirá apenas as VMs que podem ser hibernadas.

4. Siga as instruções na tela para concluir todas as configurações. A página **Resumo** exibe o status de hibernação do catálogo.

> **Nota:**
>
> Ao editar o catálogo de máquinas, quando você altera o perfil da máquina para um habilitado para hibernação, será solicitado que você reconfigure suas VMs de acordo.

Atualizar catálogo de máquinas que suporta hibernação

Se você tentar atualizar um catálogo de máquinas existente com um catálogo de máquinas que não suporta hibernação, a atualização falhará com uma mensagem de erro apropriada.

Gerenciamento de energia de VMs hibernadas

Você pode realizar as seguintes operações de gerenciamento de energia nas VMs hibernadas:

1. Suspender a VM do estado de execução.
2. Retomar a VM do estado suspenso.
3. Reiniciar a VM do estado suspenso.

Para ver as opções de gerenciamento de energia, no Studio, clique com o botão direito do mouse nas VMs hibernadas.

Você também pode ver o estado de energia como **Suspensão** e **Suspenso** para cada VM, de acordo com as operações de energia que você executa nas VMs.

Gerenciar energia de VMs do Azure

Para obter informações sobre as permissões necessárias, consulte Permissões do Azure necessárias.

Provisionamento sob demanda do Azure

Com o provisionamento sob demanda do Azure, as VMs são criadas somente quando o Citrix DaaS™ inicia uma ação de inicialização, após a conclusão do provisionamento.

Ao usar o MCS para criar catálogos de máquinas no Azure Resource Manager, o recurso de provisionamento sob demanda do Azure:

- Reduz seus custos de armazenamento
- Oferece criação de catálogo mais rápida

Ao criar um catálogo MCS, o portal do Azure exibe os grupos de segurança de rede, interfaces de rede, imagens base e discos de identidade nos grupos de recursos.

O portal do Azure não mostra uma VM até que o Citrix DaaS inicie uma ação de inicialização para ela. Em seguida, o status da VM no Studio muda para **Ativado**. Existem dois tipos de máquinas com as seguintes diferenças:

- Para uma máquina agrupada, o disco do sistema operacional e o cache de write-back existem apenas quando a VM existe. Ao desligar uma máquina agrupada no console, a VM não fica

visível no portal do Azure. Há uma economia significativa de custos de armazenamento se você desligar as máquinas rotineiramente (por exemplo, fora do horário de trabalho).

- Para uma máquina dedicada, o disco do sistema operacional é criado na primeira vez que a VM é ligada. A VM no portal do Azure permanece no armazenamento até que a identidade da máquina seja excluída. Ao desligar uma máquina dedicada no console, a VM ainda fica visível no portal do Azure.

> **Nota:**
>
> O suporte para catálogos do Azure criados antes do recurso de provisionamento sob demanda (catálogos “legados”) foi descontinuado. Portanto, recrie as VMs do catálogo legado do Azure. Os catálogos são então provisionados sob demanda, o que economiza custos de armazenamento.

Preservando uma máquina virtual provisionada ao reiniciar

Escolha se deseja preservar uma máquina virtual provisionada ao reiniciar. Use o parâmetro PowerShell `New-ProvScheme CustomProperties`. Este parâmetro suporta uma propriedade extra, `PersistVm`, usada para determinar se uma máquina virtual provisionada persiste quando reiniciada. Defina a propriedade `PersistVm` como **true** para manter uma máquina virtual quando desligada, ou defina a propriedade como **false** para garantir que a máquina virtual não seja preservada quando desligada.

> **Nota:**
>
> A propriedade `PersistVm` se aplica apenas a um esquema de provisionamento com as propriedades `CleanOnBoot` e `UseWriteBackCache` habilitadas. Se a propriedade `PersistVm` não for especificada para máquinas virtuais não persistentes, elas são excluídas do ambiente do Azure quando desligadas.

> No exemplo a seguir, o parâmetro `New-ProvScheme CustomProperties` define a propriedade `PersistVm` como **true**:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>
```

No exemplo a seguir, o parâmetro `New-ProvScheme CustomProperties` preserva o cache de write-back definindo `PersistVM` como **true**:

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"
```

```
 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

Dica:

A propriedade `PersistVm` determina se uma máquina virtual provisionada deve ser preservada. A propriedade `PersistOsdisk` determina se o disco do SO deve ser persistido. Para preservar uma máquina virtual provisionada, preserve o disco do SO primeiro. Você não pode excluir o disco do SO sem antes excluir a máquina virtual. Você pode usar a propriedade `PersistOsdisk` sem especificar o parâmetro `PersistVm`.

Personalizar o comportamento de ligar em caso de falha na alteração do tipo de armazenamento

Ao ligar, o tipo de armazenamento de um disco gerenciado pode falhar ao mudar para o tipo desejado devido a uma falha no Azure. Nesses cenários, a VM permaneceria desligada com uma mensagem de falha enviada a você. No entanto, você pode optar por ligar a VM mesmo quando o armazenamento não puder ser restaurado para o tipo configurado ou optar por manter a VM desligada.

- Se você configurar a propriedade personalizada `FailSafeStorageType` como **true** (configuração padrão) ou não a especificar nos comandos `New-ProvScheme` ou `Set-ProvScheme`:
  - Ao ligar, a VM liga com o tipo de armazenamento incorreto.
  - Ao desligar, a VM permanece desligada com o tipo de armazenamento incorreto.
- Se você configurar a propriedade personalizada `FailSafeStorageType` como **false** nos comandos `New-ProvScheme` ou `Set-ProvScheme`:
  - Ao ligar, a VM permanece desligada com o tipo de armazenamento incorreto.
  - Ao desligar, a VM permanece desligada com o tipo de armazenamento incorreto.

Para criar um catálogo de máquinas para incluir a propriedade personalizada `FailSafeStorageType`:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar os módulos PowerShell específicos da Citrix.
3. Crie um pool de identidades, se ainda não tiver sido criado.
4. Adicione a propriedade personalizada em `New-ProvScheme`. Por exemplo:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
```

```
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. Crie o catálogo de máquinas.

Para atualizar um catálogo de máquinas existente para incluir a propriedade personalizada `FailSafeStorageType`. Esta atualização não afeta as VMs existentes.

1. Atualize a propriedade personalizada no comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />

</CustomProperties>"
```

Para aplicar a alteração feita em Set-ProvScheme às VMs existentes, execute o comando `Request-ProvVMUpdate`.

1. Execute o comando Request-ProvVMUpdate. Por exemplo:

```
Request-ProvVMUpdate -ProvisioningSchemeName <String> -VMName <List-Of-
Vm-Names>
```

2. Reinicie as VMs.

Criar VMs com capacidade de hibernação

Em ambientes Azure, você pode criar um catálogo de máquinas MCS que suporta hibernação. Usando este recurso, você pode suspender uma VM e, em seguida, reconectar-se ao estado anterior da VM quando um usuário fizer login novamente.

A capacidade de hibernação aplica-se ao seguinte:

- SO de sessão única
- VMs persistentes e não persistentes
- Desktops VDI estáticos e aleatórios (agrupados)

Você pode retomar a mesma sessão depois de hibernar uma VM, independentemente de o desktop VDI ser estático ou aleatório.

Nesta seção, consulte o seguinte:

- Pré-requisitos
- Limitações
- Criar e gerenciar um catálogo de máquinas com capacidade de hibernação
- Criar um catálogo de máquinas para VMs existentes com capacidade de hibernação
- Verificar a propriedade de hibernação
- Gerenciamento de energia de VMs (Manual e Automatizado)

Pré-requisitos para usar a hibernação

Para usar a hibernação, certifique-se de concluir as seguintes tarefas:

- Instale o Agente de VM do Azure na imagem mestre para Windows e Linux. O arquivo de paginação da imagem do Windows pode estar no disco temporário. O MCS define o local do arquivo de paginação para a unidade C: no disco base quando a hibernação é ativada no catálogo de máquinas.
- O MCS define automaticamente a propriedade de hibernação para os recursos gerados. Você não precisa configurar as propriedades dos recursos mestre para oferecer suporte à hibernação.
- Use um tamanho de VM em sua assinatura que suporte a hibernação.
- Crie um perfil de máquina com capacidade de hibernação (VM ou especificação de modelo) para que as VMs herdem a capacidade de hibernação. Para criar a VM, consulte Introdução à hibernação.

> **Nota:**
>
> De acordo com a Microsoft, você pode implantar VMs com hibernação habilitada a partir de um disco de SO. Este recurso é atualmente suportado para certas regiões e estará disponível para todas as regiões em breve. Para mais informações, consulte Implantar VMs com hibernação habilitada a partir de um disco de SO.

Para criar a especificação do modelo, faça o seguinte:

a. Abra o Portal do Azure. Escolha uma VM cuja configuração você deseja usar no modelo. Selecione **Exportar modelo** no painel esquerdo.
b. Desmarque a caixa de seleção **Incluir parâmetros**. Copie o contexto e salve-o como um arquivo JSON, por exemplo, `VMExportTemplate.json`.
c. Certifique-se de que o parâmetro `hibernationEnabled` esteja `true` no modelo. Se o parâmetro não estiver `true`, verifique a configuração da VM que você usou. Você pode especificar um tamanho de VM suportado no arquivo de modelo. No entanto, você também pode especificar o tamanho da máquina ao criar o catálogo.
d. Adicione o modelo para o recurso de interface de rede ao arquivo JSON `VMExportTemplate.json`. Como resultado, você terá um arquivo de modelo ARM com dois recursos.
e. Selecione **Portal do Azure > Especificações de modelo > Importar modelo > Escolher arquivo de modelo local** para importar este arquivo de modelo como uma especificação de modelo ARM.
f. Após a criação da especificação do modelo ARM, você pode usá-la como um perfil de máquina.

> **Nota:**
>
> Pode levar alguns minutos para sincronizar com o Citrix Studio.

Para mais informações, consulte o documento da Microsoft Pré-requisitos para usar a hibernação.

Limitações

- Apenas catálogos de máquinas de SO de sessão única (persistentes e não persistentes) são suportados.
- Discos de SO efêmeros e recursos de E/S do MCS não suportam a hibernação do Azure.
- A hibernação pode falhar durante as atualizações automáticas do Windows.
- O Trusted Launch é um pré-requisito para a hibernação quando o Hyper-V está ativado.

Para obter mais informações, consulte o documento da Microsoft.

Criar e gerenciar um catálogo de máquinas com capacidade de hibernação

Para criar VMs com capacidade de hibernação, você pode criar e gerenciar um catálogo de máquinas com capacidade de hibernação usando:

- Studio
- Comandos do PowerShell

CRIAR UM CATÁLOGO USANDO O STUDIO

1. Faça login no Citrix Cloud.
2. No bloco **DaaS**, clique em **Gerenciar** para abrir o Studio.
3. No painel esquerdo, selecione **Catálogos de Máquinas**.
4. Selecione **Criar Catálogo de Máquinas**. O assistente de criação de catálogo será aberto.
5. Na página **Tipo de Máquina**, selecione o tipo de máquina **SO de sessão única** para este catálogo.
6. Na página **Gerenciamento de Máquinas**, selecione as configurações da seguinte forma:
    a. Selecione **Máquinas com gerenciamento de energia (por exemplo, máquinas virtuais ou PCs blade)**.
    b. Selecione **Citrix Machine Creation Services™ (MCS)**.
    c. Selecione um local de recurso na lista suspensa **Recursos**.
7. Na página **Experiência da Área de Trabalho**, selecione a experiência da área de trabalho aleatória ou estática conforme necessário.
8. Na página **Imagem**, selecione uma imagem mestre. Marque a caixa de seleção **Usar um perfil de máquina** e selecione um perfil de máquina que suporte hibernação. Clique na dica de ferramenta para saber se um perfil de máquina suporta hibernação.

> **Nota:**
>
> Se você selecionar uma imagem mestre gerenciada pelo Azure, somente as imagens na mesma região do local de recurso selecionado serão exibidas.

9. Na página **Tipos de Armazenamento e Licença**, selecione o armazenamento e a licença a serem usados para este catálogo.
10. Na página **Máquinas Virtuais**, selecione a contagem de VMs, o tamanho da VM e a zona de disponibilidade.

> **Nota:**
>
> Os tamanhos de máquina que suportam hibernação são mostrados apenas para sua seleção.

11. Na página **NICs**, adicione as NICs que você deseja que as VMs usem.
12. Na página **Configurações de Disco**, selecione o tipo de armazenamento e o tamanho do disco de cache de write-back.
13. Na página **Grupo de Recursos**, selecione o grupo de recursos para provisionar VMs.
14. Na página **Identidades da Máquina**, selecione **Criar novas contas do Active Directory**. Em seguida, especifique um esquema de nomenclatura de conta.
15. Na página **Credenciais de Domínio**, clique em **Inserir credenciais**. Insira suas credenciais de domínio para realizar a criação da conta no domínio do Active Directory de destino.
16. Na página **Resumo**, insira um nome para o catálogo de máquinas e clique em **Concluir**.

Quando a criação do catálogo de máquinas MCS estiver concluída, localize o catálogo na lista de catálogos e clique na guia **Propriedades do Modelo**. O valor do parâmetro **Hibernação** deve ser **Suportado**.

Se você quiser editar um catálogo de máquinas, considere as seguintes restrições:

- Se o catálogo de máquinas atual suportar hibernação, você não pode:
  - Alterar o tamanho da VM para um que não seja capaz de hibernar.
  - Alterar o perfil da máquina para um que não seja capaz de hibernar.

- Se o catálogo de máquinas atual não suportar hibernação, você não pode:
    - atualmente, alterar o perfil da máquina para um que seja capaz de hibernar usando o Studio.

CRIAR UM CATÁLOGO DE MÁQUINAS PARA GERENCIAR VMS EXISTENTES CAPAZES DE HIBERNAR

Se você já tiver VMs capazes de hibernar e quiser suspendê-las e retomá-las, crie um catálogo de máquinas para importar essas VMs para gerenciamento de energia.

> **Nota:**
>
> Você pode criar um catálogo de máquinas contendo VMs capazes e incapazes de hibernar. No entanto, se você quiser funcionalidade relacionada à hibernação, você deve criar o catálogo de máquinas apenas com VMs capazes de hibernar.

> Para criar um catálogo para VMs existentes capazes de hibernar usando o Studio, siga as instruções na tela para concluir as etapas e preste atenção às seguintes configurações principais:

1. Na página **Gerenciamento de Máquinas**, selecione **Máquinas com gerenciamento de energia** e, em seguida, selecione **Outro serviço ou tecnologia** como a forma de implantar máquinas.
2. Na página **Máquinas Virtuais**, adicione ou importe apenas as VMs capazes de hibernar.

CRIAR UM CATÁLOGO DE MÁQUINAS USANDO COMANDOS DO POWERSHELL

Depois de atender a todos os requisitos para usar a hibernação, você pode criar um catálogo de máquinas com capacidade de hibernação usando o comando `New-ProvScheme`. Para obter informações sobre como criar um catálogo usando o SDK do PowerShell Remoto, consulte Gerenciar Citrix DaaS usando SDKs do PowerShell Remoto.

Ao criar o catálogo, você pode verificar se um tamanho de VM e um perfil de máquina suportam hibernação ou não usando os seguintes comandos do PowerShell:

- Para o tamanho da VM, execute o seguinte comando e verifique se a propriedade `supportsHibernation` é **True**. Por exemplo,

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <VirtualNetwork>
\serviceoffering.folder") | select Name, AdditionalData | ConvertTo-
Json
```

- Para o perfil da máquina, execute o seguinte comando e verifique se a propriedade `supportsHibernation` é **True**. Por exemplo,

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

Se você quiser editar um catálogo de máquinas, considere as seguintes restrições:

- Se o catálogo de máquinas atual suportar hibernação, você não pode:
  - Alterar o tamanho da VM para um que não seja capaz de hibernar
  - Alterar o perfil da máquina para um que não seja capaz de hibernar
- Se o catálogo de máquinas atual não suportar hibernação, você não pode:
  - atualmente, alterar o perfil da máquina para um que seja capaz de hibernar usando o Studio.

Para obter informações sobre como modificar o tamanho da VM e o perfil da máquina de um catálogo usando o SDK do PowerShell Remoto, consulte `<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`.

Verificar a propriedade de hibernação

Você pode verificar a propriedade de hibernação de um catálogo de máquinas, VM e uma máquina broker usando os comandos do PowerShell:

- Para verificar a propriedade de hibernação de um esquema de provisionamento, execute os seguintes comandos do PowerShell. O parâmetro `HibernationEnabled` deve ser `True`.

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- Para verificar a propriedade de hibernação de uma VM de provisionamento, execute os seguintes comandos PowerShell. O parâmetro `SupportsHibernation` deve ser `True`.

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- Para verificar a capacidade de hibernação de uma máquina broker, execute os seguintes comandos PowerShell. As ações de energia **Suspender** e **Retomar** indicam capacidade de hibernação.

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

Gerenciamento de energia de VMs com capacidade de hibernação

Você pode realizar as seguintes operações de gerenciamento de energia nas VMs com capacidade de hibernação:

- **Suspender** VM do estado de execução
- **Retomar** VM do estado suspenso
- **Forçar desligamento** da VM de um estado suspenso
- **Forçar reinício** da VM do estado suspenso

Consulte o seguinte para obter mais informações:

- Suspender
- Retomar

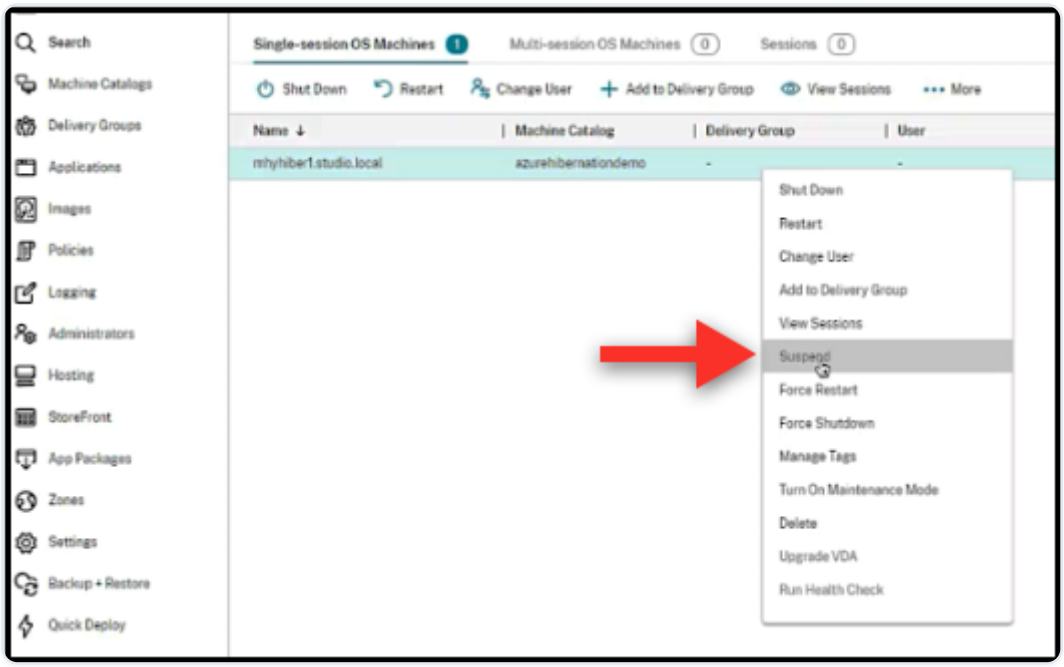
SUSPENDER

Você pode suspender uma VM usando uma das seguintes maneiras:

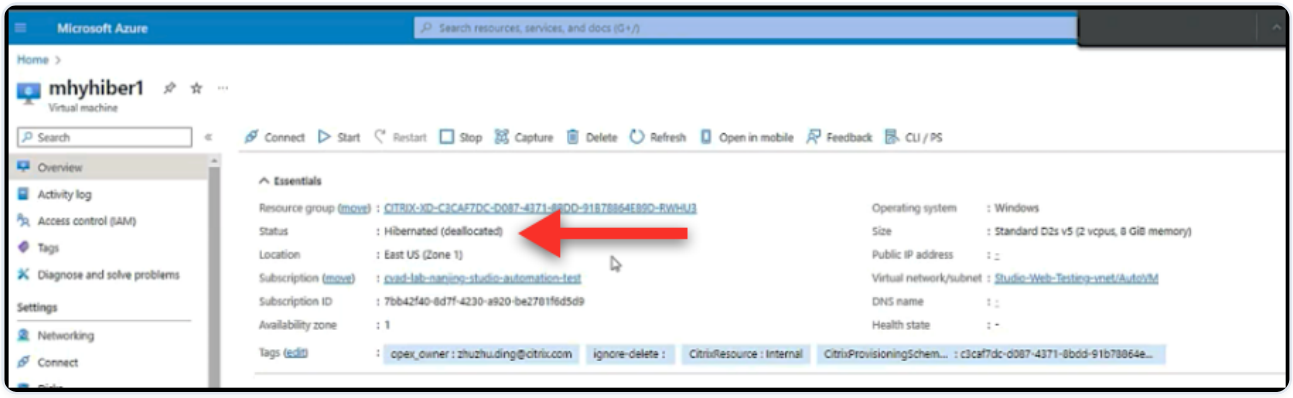
- **Manualmente** usando o Studio
- **Automaticamente** usando a política de tempo limite: Para obter mais informações, consulte Configurações diversas.

Para suspender manualmente uma VM:

1. Clique com o botão direito na VM e selecione **Suspender**. Clique em **Sim** para confirmar a ação. O **Estado de Energia** muda de **Suspensão** para **Suspenso**.



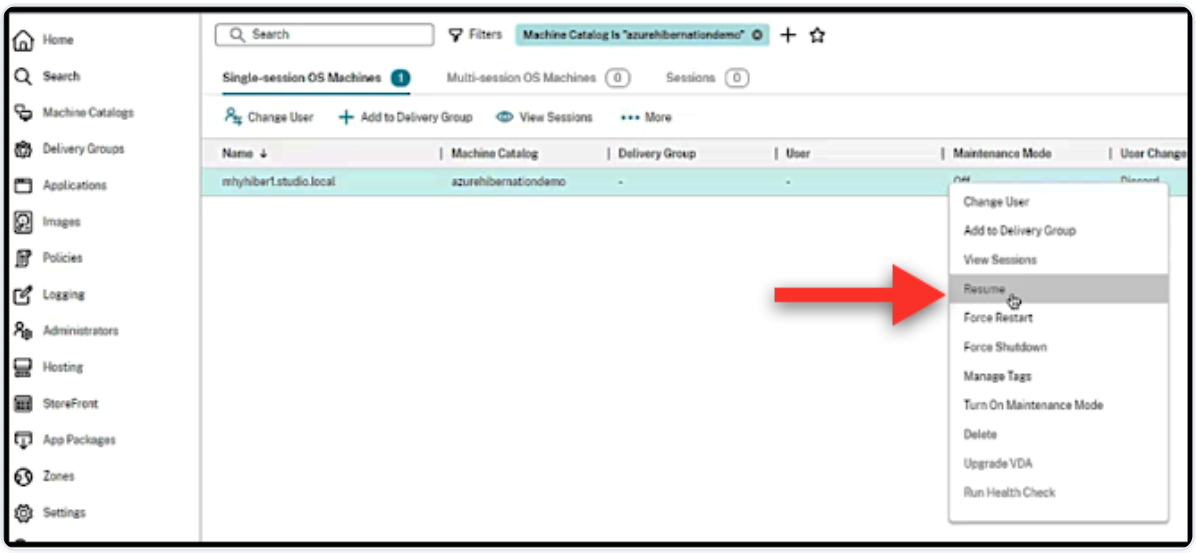
Você pode verificar o status da VM no portal do Azure.



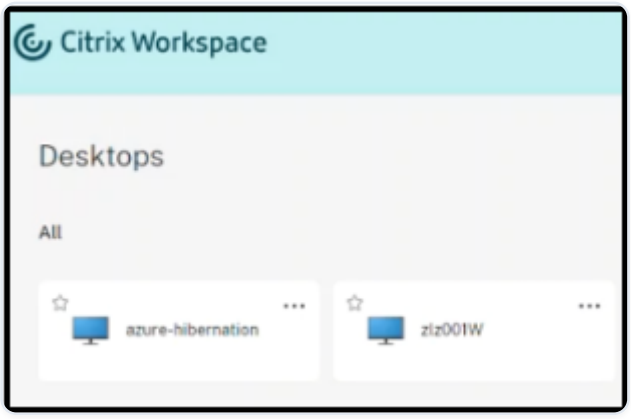
RETOMAR

Para retomar uma VM hibernada, use uma das seguintes maneiras:

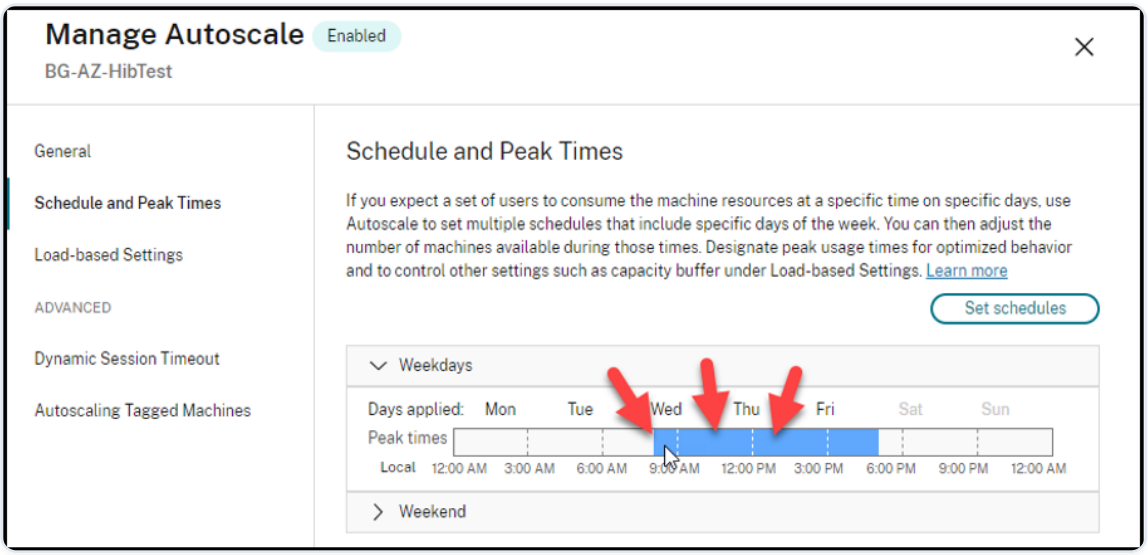
- **Manualmente**:
  - Os administradores podem retomar a VM usando o Studio.



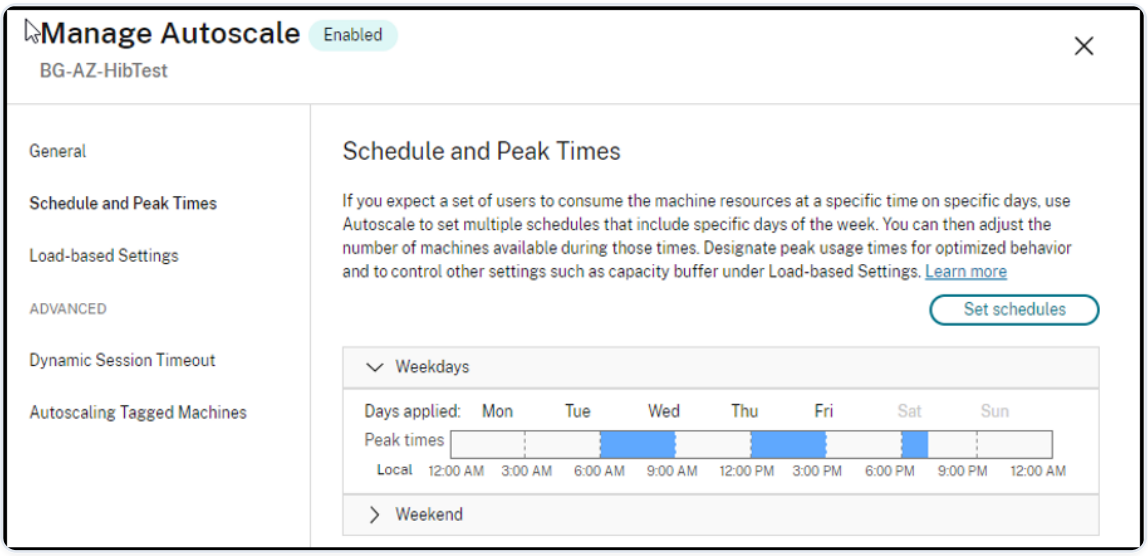
- Quando os usuários finais iniciam a área de trabalho, ela é retomada automaticamente.



- **Automaticamente**:
  - O Autoscale™ pode ligar automaticamente as máquinas hibernadas se você configurar os horários de pico corretamente. Você pode definir os horários de pico em intervalos de 30 minutos clicando na programação de horários. Cada quadro azul representa um slot de tempo marcado como horário de pico. Os horários de pico podem ter slots de tempo consecutivos e não consecutivos.
    - Slots de tempo consecutivos

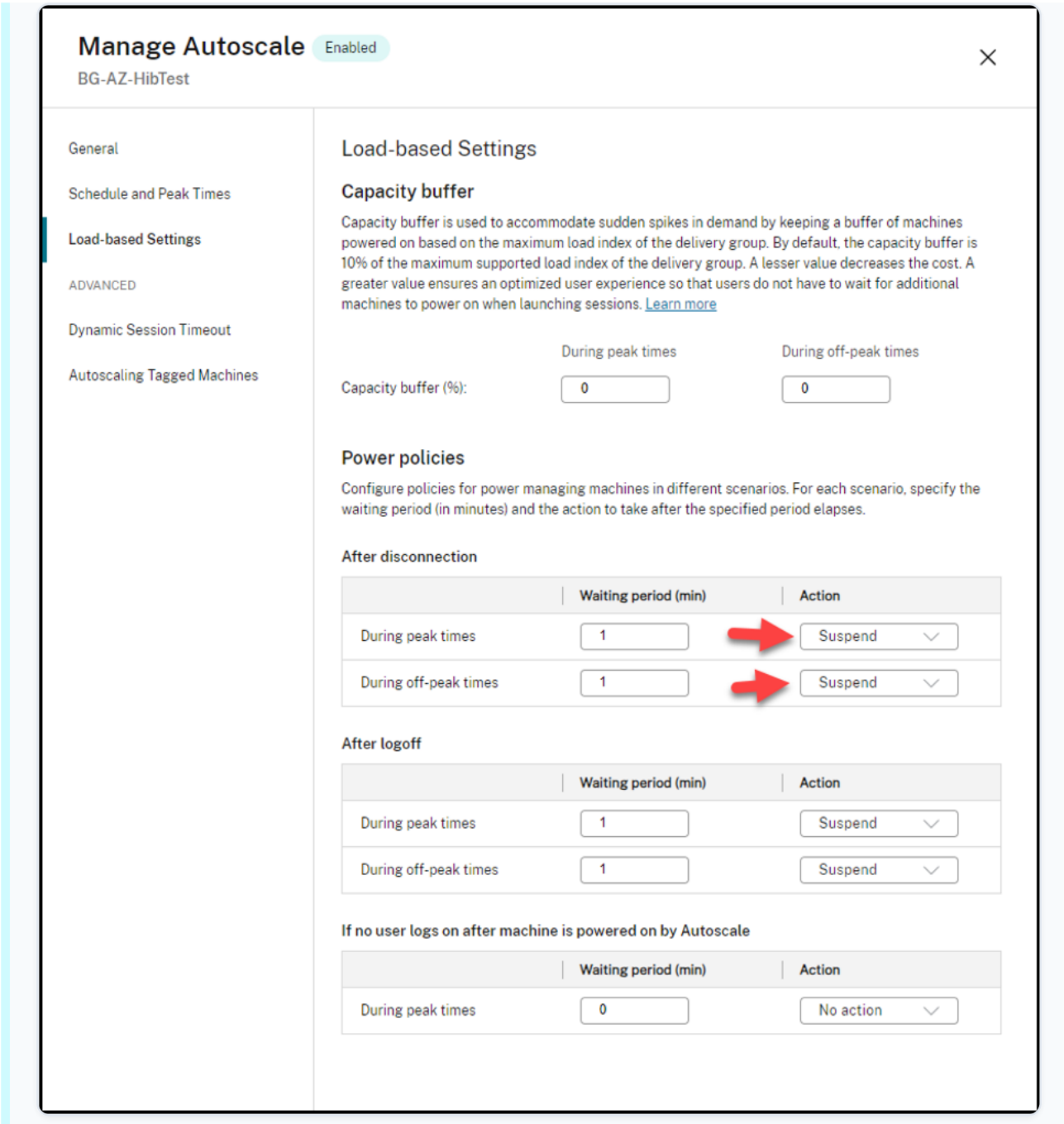


- Slots de tempo não consecutivos



Nota:

Em **Gerenciar Autoescala > Configurações baseadas em carga**, se a **Ação** estiver configurada como **Suspender**, então certifique-se de que todas as VMs dentro desse grupo de entrega tenham capacidade de hibernação. Caso contrário, as VMs que não podem hibernar continuarão a ser executadas.



Obter mensagens de aviso para falha de hibernação

Você pode obter mensagens de aviso usando um comando PowerShell `Get-ProvOperationEvent` em caso de falha de hibernação de VMs provisionadas por MCS e VMs existentes com capacidade de hibernação. Para obter informações sobre o comando Powershell, consulte a documentação do SDK Get-ProvOperationEvent.

Para fazer isso:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*` para carregar módulos PowerShell específicos da Citrix.

3. Execute `Get-ProvOperationEvent` para obter a mensagem de aviso em caso de falha de hibernação.

```
Get-ProvOperationEvent -filter { OperationName -eq "Suspend" }
```

Saída:

```
EventAdditionalData : Error code = OperationNotAllowed and Error
message = The Hibernate-Deallocate Operation cannot be performed on a
VM that has extension 'AzureHibernateExtension' in failed state. For
more information, see https://aka.ms/hibernate-resume/errors. Error
details from the extension : Enabling

                  hibernate failed. Response from the powercfg command.
Exit Code: 1. Error message:

                  Hibernation failed with the following error: The
request is not supported.



                  The following items are preventing hibernation on
this system.

                    The current Device Guard configuration has disabled
hibernation.

                    An internal system component has disabled
hibernation.

                            Hypervisor

                  Status: 409

                  ErrorCode: OperationNotAllowed



                  Content:

                  {
```

```
                    "error": {

                      "code": "OperationNotAllowed",

                      "message": "The Hibernate-Deallocate Operation
cannot be performed on a VM that has extension
'AzureHibernateExtension' in failed state. For more information, see
https://aka.ms/hibernate-resume/errors. Error details from the
extension : Enabling hibernate failed. Response from the

                  powercfg command. Exit Code: 1. Error message:
\nHibernation failed with the following error: The request is not
supported.\r\n\r\nThe following items are preventing hibernation on
this system.\r\n\tThe current Device Guard configuration has disabled
hibernation.\r\n\tAn internal system

                  component has disabled hibernation.
\r\n\t\tHypervisor"

                    }

                  }

EventCategory       : Warning

EventDateTime       : 1/11/2024 4:18:31 AM

EventId             : 0

EventMessage        : Failed to suspend machine my-resource-group/my-
vm.

EventSeverity       : Important

EventSource         : AzureRmPlugin

EventState          : New

LinkedObjectType    : ProvisioningScheme

LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366

OperationName       : Suspend
```

```
OperationTargetName : my-resource-group/my-vm

OperationTargetType : VirtualMachine

OperationType       : PowerManagement

Recommendation      :
```

SOLUÇÃO DE PROBLEMAS DE HIBERNAÇÃO

Você recebe a seguinte mensagem de erro se você tentar habilitar os recursos de hibernação e de VM de inicialização confiável, no entanto, a configuração do sistema operacional convidado não está correta.

CÓDIGO DE ERRO	MENSAGEM DE ERRO
OperationNotAllowed	A Operação de Hibernar-Desalocar não pode ser realizada em uma VM que tenha a extensão 'AzureHibernateExtension' em estado de falha. Para obter mais informações, consulte `<https://aka.ms/hibernate-resume/errors/>`. Detalhes do erro da extensão: A habilitação da hibernação falhou. Resposta do comando powercfg. Código de Saída: 1. Mensagem de erro: A hibernação falhou com o seguinte erro: A solicitação não é suportada. Os seguintes itens estão impedindo a hibernação neste sistema. **A configuração atual do Device Guard desativou a hibernação. Um componente interno do sistema desativou a hibernação**.

Para resolver o problema, certifique-se de que a virtualização esteja habilitada na VM convidada. Por exemplo, confirme se o Hyper-V está habilitado em um ambiente Windows.

Para obter mais informações sobre mensagens de aviso, consulte o documento da Microsoft Solução de problemas de hibernação de VM.

Nota:

> Mensagens de erro relacionadas à falha na retomada de uma VM estarão disponíveis em uma versão futura.

Mais informações

Para obter mais informações sobre a hibernação do Citrix Azure, consulte o artigo da Citrix Tech Zone.

Gerenciar energia de VMs Nutanix AHV

Com o Citrix DaaS™, você pode gerenciar a energia de VMs Nutanix AHV. Use o nó **Pesquisar** no painel de navegação para encontrar a máquina que deseja gerenciar.

Você pode usar as seguintes ações de energia:

- Iniciar
- Desligar
- Desligamento Forçado
- Reinicialização Forçada
- Reiniciar

> **Nota:**
>
> - As ações de energia Redefinir, Suspender e Retomar não são suportadas.
> - Desligar ou Reiniciar: A VM pode não responder à solicitação de desligamento se usuários ativos ou programas em execução interromperem o desligamento, ou se o sistema operacional exigir atualizações. Para garantir que o desligamento e a reinicialização do convidado funcionem corretamente em VMs Windows, aplique as configurações de ação de energia recomendadas no VDA, como configurações de protetor de tela e energia de exibição. Para obter mais informações, consulte Nutanix KB.

Políticas de segurança

Este artigo descreve os recursos de segurança em vários hipervisores suportados. Os recursos de segurança incluem:

- Grupo de segurança
- Inicialização segura
- Recursos de criptografia

Grupo de segurança

Grupo de segurança é um grupo de regras de segurança para filtrar o tráfego de rede entre recursos em uma rede virtual. As regras de segurança permitem ou negam o tráfego de rede de entrada para, ou o tráfego de rede de saída de, vários tipos de recursos. Cada regra especifica as seguintes propriedades:

- Nome: Um nome exclusivo dentro do grupo de segurança de rede
- Prioridade: As regras são processadas em ordem de prioridade, com números menores sendo processados antes de números maiores, porque números menores têm prioridade mais alta
- Origem ou Destino: Qualquer, ou um endereço IP individual, bloco de roteamento entre domínios sem classe (CIDR) (10.0.0.0/24, por exemplo), tag de serviço ou grupo de segurança de aplicativo
- Protocolo: Os protocolos com base nos quais você adiciona regras para cada grupo de segurança
- Direção: Se a regra se aplica ao tráfego de entrada ou de saída
- Intervalo de portas: Você pode especificar uma porta individual ou um intervalo de portas
- Ação: Permitir ou negar

Consulte o seguinte para obter mais informações sobre hipervisores suportados:

- Grupo de segurança na AWS
- Grupo de segurança no Microsoft Azure
- Grupo de segurança no Google Cloud Platform

Grupo de segurança na AWS

Grupos de segurança atuam como firewalls virtuais que controlam o tráfego para as instâncias em sua VPC. Você adiciona regras aos seus grupos de segurança que permitem que as instâncias em sua sub-rede pública se comuniquem com as instâncias em sua sub-rede privada. Você também pode associar esses grupos de segurança a cada instância em sua VPC. As regras de entrada controlam o tráfego que chega à sua instância, e as regras de saída controlam o tráfego que sai da sua instância.

Para mais informações sobre a configuração de rede durante a preparação da imagem, consulte Configuração de rede durante a preparação da imagem.

Ao iniciar uma instância, você pode especificar um ou mais grupos de segurança. Para configurar grupos de segurança, consulte Configurar grupos de segurança.

Grupo de segurança no Microsoft Azure

O Citrix DaaS oferece suporte a grupos de segurança de rede no Azure. Espera-se que os grupos de segurança de rede se associem a sub-redes. Para obter mais informações, consulte Grupos de segurança de rede.

Para obter mais informações sobre o grupo de segurança de rede criado durante a preparação da imagem, consulte Criar um catálogo de máquinas usando uma imagem do Azure Resource Manager.

Grupo de segurança no Google Cloud Platform

Durante a preparação de um catálogo de máquinas, uma imagem de máquina é preparada para servir como disco do sistema da imagem mestre para o catálogo. Quando esse processo ocorre, o disco é temporariamente anexado a uma máquina virtual. Esta VM deve ser executada em um ambiente isolado que impede todo o tráfego de rede de entrada e saída. Isso é realizado por meio de um par de regras de firewall de negação total. Para obter mais informações, consulte Regras de Firewall.

Inicialização Segura e vTPM

A Inicialização Segura é um recurso da Unified Extensible Firmware Interface (UEFI), que é responsável pela inicialização do sistema. Ela garante que apenas software confiável seja carregado durante o processo de inicialização.

Trusted Platform Module (TPM) é um chip de hardware que fornece armazenamento seguro para chaves criptográficas e outros dados confidenciais. Um Virtual Trusted Platform Module (vTPM) executa as mesmas funções que um TPM, mas executa recursos de coprocessador criptográfico em software. Embora o TPM possa aumentar a segurança, ele não é um requisito para a Inicialização Segura.

Consulte o seguinte para obter mais informações sobre hipervisores suportados:

- Inicialização Segura e NitroTPM no AWS
- Inicialização Segura e vTPM no Google Cloud Platform
- Inicialização Segura e vTPM no Microsoft Azure

- Inicialização Segura e vTPM no Nutanix Prism Central
- vTPM no VMware
- Inicialização Segura e vTPM para XenServer
- Inicialização Segura e vTPM no SCVMM

Inicialização Segura e NitroTPM no AWS

Em ambientes AWS, você pode selecionar uma imagem mestre (AMI) com NitroTPM e/ou inicialização segura UEFI habilitados. Consequentemente, as VMs provisionadas no catálogo também são habilitadas com NitroTPM e/ou inicialização segura UEFI. Essa implementação garante que as VMs sejam seguras e confiáveis. Para obter mais informações sobre NitroTPM e Inicialização Segura UEFI, consulte a documentação da Amazon. Para criar um catálogo habilitado com NitroTPM e inicialização segura UEFI, consulte Habilitar NitroTPM e inicialização segura UEFI para instâncias de VM.

Inicialização Segura e vTPM no Google Cloud Platform

Você pode provisionar máquinas virtuais blindadas no Google Cloud Platform (GCP). A integridade verificável da VM blindada é alcançada usando os seguintes recursos:

- Inicialização Segura
- Inicialização Medida habilitada para vTPM
- Monitoramento de integridade

Para obter mais informações sobre como usar o PowerShell para criar um catálogo com VM blindada, consulte Usando o PowerShell para criar um catálogo com VM blindada.

> **Nota:**
>
> Se você instalar o Windows 11 na imagem mestre, deverá habilitar o vTPM durante o processo de criação da imagem mestre. Além disso, se você usar um perfil de máquina para criar o catálogo, deverá habilitar o vTPM na origem do perfil de máquina (VM ou modelo de instância). Para obter informações sobre como criar VMs do Windows 11 no nó de locatário único, consulte Criar VMs do Windows 11 no nó de locatário único.

Inicialização Segura e vTPM no Microsoft Azure

Em ambientes Azure, você pode criar catálogos de máquinas habilitados com Inicialização Confiável. O Azure oferece a Inicialização Confiável como uma maneira contínua de melhorar a

segurança das VMs de geração 2. A Inicialização Confiável protege contra técnicas de ataque avançadas e persistentes. Para habilitar a Inicialização Confiável, use uma configuração de catálogo baseada em perfil de máquina. Na raiz da Inicialização Confiável está a Inicialização Segura para sua VM. A Inicialização Confiável também usa o vTPM para realizar atestado remoto pela nuvem. Isso é usado para verificações de integridade da plataforma e para tomar decisões baseadas em confiança. Você pode habilitar individualmente a Inicialização Segura e o vTPM. Para obter mais informações sobre como criar um catálogo de máquinas com Inicialização Confiável, consulte Catálogos de máquinas com Inicialização Confiável.

Inicialização Segura e vTPM no Nutanix Prism Central

O MCS oferece suporte à criação de um catálogo de máquinas com vTPM, UEFI e inicialização segura com o Nutanix Prism Central. Você pode selecionar uma imagem mestre (modelo) com vTPM e inicialização segura UEFI habilitados.

No Nutanix Prism Central, a Inicialização Segura UEFI não requer vTPM. No entanto, para vincular um vTPM a uma VM, a VM deve ser inicializada por UEFI, independentemente de a Inicialização Segura estar habilitada ou não.

Além disso, VMs habilitadas para vTPM, UEFI e inicialização segura podem ser importadas do Nutanix Prism Central e podem ser gerenciadas por energia pelo Citrix DaaS.

A Nutanix oferece suporte para vTPM e Inicialização Segura UEFI. Consulte:

- Suporte a vTPM (Módulo de Plataforma Confiável Virtual) no AHV.
- Suporte à Inicialização Segura para VMs
- Protegendo VMs AHV com um Módulo de Plataforma Confiável Virtual

vTPM no VMware

O MCS oferece suporte à criação de um catálogo de máquinas com vTPM. Se o Windows 11 estiver instalado na imagem mestre, é um requisito ter o vTPM habilitado para a imagem mestre. Se a configuração baseada em perfil de máquina for usada e o vTPM estiver habilitado, as VMs no catálogo herdarão o mesmo conteúdo vTPM do modelo de VM. Se o perfil de máquina não for usado e a imagem mestre tiver o vTPM habilitado, as VMs no catálogo terão o vTPM em branco. Para obter mais informações, consulte Criar um catálogo de máquinas usando um perfil de máquina.

Secure Boot e vTPM para XenServer®

O XenServer oferece UEFI Secure Boot em alguns de seus sistemas operacionais de VM suportados. O Secure Boot impede que binários não assinados, assinados incorretamente ou modificados sejam executados durante a inicialização. Em uma VM habilitada para UEFI que impõe o Secure Boot, todos os drivers devem ser assinados. Para obter mais informações, consulte UEFI de convidado e Secure Boot.

No XenServer 8, o vTPM não é necessário para o UEFI Secure Boot. No entanto, para vincular um vTPM a uma VM, essa VM deve ser inicializada por UEFI, independentemente de o Secure Boot estar habilitado ou não. A VM do Windows 11 requer um vTPM vinculado e ele é criado automaticamente quando a VM do Windows 11 é criada a partir do modelo fornecido. Para outros sistemas operacionais, um vTPM é opcional. Para obter mais informações, consulte vTPM.

O MCS oferece suporte à criação de um catálogo de máquinas com vTPM. Se a configuração baseada em perfil de máquina for usada e o vTPM estiver habilitado, as VMs no catálogo herdarão o mesmo conteúdo vTPM do modelo de VM. Se o perfil de máquina não for usado e a imagem mestre tiver o vTPM habilitado, as VMs no catálogo herdarão o mesmo conteúdo vTPM da imagem mestre.

Secure Boot e vTPM no SCVMM

Em ambientes do System Center Virtual Machine Manager (SCVMM), você pode selecionar uma imagem mestre e um perfil de máquina com vTPM e/ou Secure Boot habilitados. Como resultado, o catálogo provisiona VMs com vTPM e/ou Secure Boot habilitados. Essa implementação protege as VMs e as mantém confiáveis. Para criar um catálogo com vTPM e Secure Boot habilitados, consulte criar um catálogo com um perfil de máquina.

Recursos de criptografia

Os recursos de criptografia protegem o conteúdo das máquinas virtuais contra ataques de convidados mal-intencionados em um host de máquina virtual compartilhado e contra ataques lançados pelo software de controle do hipervisor que gerencia todas as máquinas virtuais no host.

Consulte o seguinte para obter mais informações sobre hipervisores suportados:

- Recursos de criptografia na AWS
- Recursos de criptografia no Google Cloud Platform
- Recursos de criptografia no Microsoft Azure

Recursos de criptografia na AWS

Esta seção descreve os recursos de criptografia em ambientes de virtualização da AWS.

Criptografia automática

Você pode ativar a criptografia automática de novos volumes Amazon EBS e cópias de snapshot criadas em sua conta. Para obter mais informações, consulte Criptografia automática.

Recursos de criptografia no Google Cloud Platform

Esta seção descreve os recursos de criptografia em ambientes de virtualização do Google Cloud Platform (GCP).

Se você precisar de mais controle sobre as operações de chave do que o permitido pelas chaves de criptografia gerenciadas pelo Google, poderá usar chaves de criptografia gerenciadas pelo cliente. Ao usar uma chave de criptografia gerenciada pelo cliente, um objeto é criptografado com a chave pelo Cloud Storage no momento em que é armazenado em um bucket, e o objeto é automaticamente descriptografado pelo Cloud Storage quando é servido aos solicitantes. Para obter mais informações, consulte Chaves de criptografia gerenciadas pelo cliente.

Você pode usar Chaves de Criptografia Gerenciadas pelo Cliente (CMEK) para catálogos MCS. Para obter mais informações, consulte Usando Chaves de Criptografia Gerenciadas pelo Cliente (CMEK).

Recursos de criptografia no Microsoft Azure

Esta seção descreve os recursos de criptografia em ambientes de virtualização do Azure.

Criptografia do lado do servidor do Azure

A maioria dos discos gerenciados do Azure é criptografada com a criptografia de Armazenamento do Azure, que usa criptografia do lado do servidor (SSE) para proteger seus dados e ajudá-lo a cumprir seus compromissos de segurança e conformidade. O Citrix DaaS oferece suporte a chaves de criptografia gerenciadas pelo cliente para discos gerenciados do Azure por meio do Azure Key Vault. Para obter mais informações, consulte Criptografia do lado do servidor do Azure.

Criptografia de disco do Azure no host

Você pode criar um catálogo de máquinas MCS com capacidade de criptografia no host.

Este método de criptografia não criptografa os dados por meio do armazenamento do Azure. O servidor que hospeda a VM criptografa os dados e, em seguida, os dados criptografados fluem

pelo servidor de armazenamento do Azure. Portanto, este método de criptografia criptografa os dados de ponta a ponta.

Para obter mais informações sobre como criar um catálogo de máquinas MCS com capacidade de criptografia no host, consulte Criptografia de disco do Azure no host.

Criptografia dupla do Azure

A criptografia dupla é a criptografia do lado da plataforma (padrão) e a criptografia gerenciada pelo cliente (CMEK). Portanto, se você é um cliente com alta sensibilidade à segurança e preocupado com o risco associado a qualquer algoritmo de criptografia, implementação ou uma chave comprometida, você pode optar por esta criptografia dupla. Discos de SO e de dados persistentes, instantâneos e imagens são todos criptografados em repouso com criptografia dupla. Para obter mais informações, consulte Criptografia dupla em disco gerenciado.

VMs confidenciais do Azure

As VMs de computação confidencial do Azure garantem que sua área de trabalho virtual seja criptografada na memória e protegida em uso.

Você pode usar o MCS para criar um catálogo com VMs confidenciais do Azure. Você deve usar o fluxo de trabalho de perfil de máquina para criar tal catálogo. Você pode usar tanto a VM quanto o modelo ARM como entrada de perfil de máquina.

Para obter mais informações, consulte VMs confidenciais do Azure.

Janela de Serviço

O recurso Janela de Serviço oferece a capacidade de agendar e automatizar operações em VMs provisionadas por MCS. Atualmente, esse recurso oferece suporte a várias operações, como redefinição de disco do sistema operacional e alterações na configuração de hardware. Você pode agendar essas operações e retornar mais tarde para verificar a conclusão, em vez de realizar as atualizações manualmente.

Você pode agendar operações para uma lista específica de VMs ou para um catálogo de máquinas inteiro. Cada operação é executada no horário especificado. Várias operações podem ser agendadas para a mesma VM. No entanto, você não pode agendar mais de uma atualização de hardware para uma única VM.

Você também pode:

- Adicionar uma descrição para a Janela de Serviço.

- Fornecer uma mensagem detalhada a ser exibida para todos os usuários que estiverem logados quando a operação for executada.
- Configurar quantos minutos de buffer são concedidos para salvar o trabalho dos usuários logados antes que a operação seja executada à força.

Vantagens

Experiência do usuário e continuidade aprimoradas

- **Tratamento de sessão elegante**: Em vez de desconexões abruptas, você pode definir uma notificação profissional para salvar o trabalho antes que a VM seja desligada.
- **Tempo de inatividade programado**: Você pode mover tarefas de atualização pesadas para horários de pico (por exemplo, 2:00 AM) sem precisar fazer login manualmente nesse horário.
- **Atualizações de hardware com custo-benefício**: A atualização de hardware usando a Janela de Serviço economiza custos significativos em grandes implementações. Esse recurso analisa automaticamente se uma VM requer uma reinicialização para aplicar as configurações. Portanto, ao evitar reinicializações desnecessárias, a Janela de Serviço minimiza essas despesas.

Flexibilidade avançada de hardware

- **Atualizar configurações de hardware**: Use a Janela de Serviço para agendar as atualizações de hardware. O sistema gerencia inteligentemente o fluxo de atualização, verificando a necessidade de reinicialização e lidando com os log-offs de sessão, garantindo que seu catálogo evolua para atender às novas demandas de recursos com supervisão manual zero.
- **Reconfiguração flexível de SKU**: Atualize facilmente os SKUs, o que antes exigia a recriação manual do catálogo.
- **Suporte à hibernação para VMs existentes**: Supera a limitação de "disco temporário". A Janela de Serviço permite que o driver MCSIO realoque o arquivo de paginação para a unidade C: e habilite as propriedades de hibernação em VMs que já foram implantadas.

Consideração importante

- **Notificação do usuário**: Usuários logados recebem um alerta inicial sobre a operação da Janela de Serviço, garantindo que tenham tempo suficiente para salvar seu trabalho. Assim que o período de notificação expira, a máquina é desligada automaticamente para realizar a operação.

Limitação

O tamanho do disco WBC não pode ser alterado nas VMs existentes. Ele pode ser aplicado ao catálogo de máquinas para as novas VMs.

Operações da Janela de Serviço

A Janela de Serviço atualmente suporta redefinições de disco do SO e alterações de configuração de hardware usando PowerShell.

Comandos PowerShell: Comandos genéricos são descritos neste artigo, enquanto scripts detalhados e específicos do hipervisor podem ser encontrados em nossa página do GitHub `<https://github.com/citrix/citrix-mcs-sdk-samples/>`.

Redefinir disco do SO

As redefinições de disco do SO podem ser feitas usando o comando PowerShell `New-ProvMaintenanceCycle`. Os comandos criam uma nova Janela de Serviço para um catálogo inteiro ou VMs específicas. O ciclo começa no horário que você especificar em `ScheduledStartTimeInUTC`. Você também fornece `MaxDurationInMinutes`, que indica o tempo máximo que a Janela de Serviço pode ser executada.

Exemplo: Redefinir disco do SO para VMs específicas

```
New-ProvMaintenanceCycle -Operation ResetOSDisk
-MaintenanceCycleDescription "Resetting Boot Disk" -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -PurgeDBAfterInDays
1 -SessionWarningTimeInMinutes 15 -SessionWarningLogOffTitle "Scheduled
Maintenance" -SessionWarningLogOffMessage "There is a scheduled
maintenance coming up and involves turning off the machine, please save
your work and log out, Thank You" -VMName VDA02,VDA03
```

Exemplo: Redefinir disco do SO para o catálogo inteiro

```
New-ProvMaintenanceCycle -Operation ResetOSDisk
-MaintenanceCycleDescription "Resetting Boot Disk" -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -PurgeDBAfterInDays
1 -SessionWarningTimeInMinutes 15 -SessionWarningLogOffTitle "Scheduled
Maintenance" -SessionWarningLogOffMessage "There is a scheduled
maintenance coming up and involves turning off the machine, please save
your work and log out, Thank You" -AllVMs
```

Atualizar configurações de hardware

Agende atualizações de hardware usando a Janela de Serviço, tendo assim controle total sobre quando as alterações entram em vigor. Você pode optar por direcionar apenas as VMs recém-criadas, um catálogo inteiro (VMs novas e existentes) ou VMs específicas, conforme necessário.

- Para atualizar as configurações de hardware para novas VMs ou para o catálogo inteiro, selecione uma versão do esquema de provisionamento e execute o comando PowerShell `New-ProvSchemeHardwareUpdate`. Você pode aplicar uma versão do esquema de provisionamento criada anteriormente às VMs. Você também pode habilitar a hibernação em uma VM com disco temporário.
- Para atualizar as configurações de hardware para VMs específicas, selecione uma versão de configuração de VM e execute o comando PowerShell `New-ProvVmHardwareUpdate`.

Considerações importantes

- Novas máquinas adicionadas a um catálogo após o agendamento de uma atualização de hardware continuam a ser criadas com especificações mais antigas até o horário UTC especificado para a aplicação de novas especificações.
- Uma única falha de validação durante a criação da Janela de Serviço impede que o ciclo seja criado e retorna uma mensagem de erro.
- Para habilitar a hibernação, considere o seguinte:
  - A versão do VDA deve ser superior a 2503.
  - O Machine Creation Services I/O (MCSIO) deve estar instalado.
  - O perfil da máquina deve suportar hibernação.
  - O SKU da VM e o sistema operacional devem suportar hibernação.
  - Se o VBS estiver habilitado, o Hyper-V também deve estar habilitado. A virtualização aninhada requer o Trusted Launch na VM.
  - O tamanho livre do disco do SO deve ser maior que o tamanho da memória da VM.

Agendar atualizações de hardware em um catálogo de máquinas inteiro ou em novas VMs

1. Execute `New-ProvSchemeVersion` para criar uma nova versão do esquema de provisionamento com configurações de hardware atualizadas. Para obter mais informações, consulte a documentação do SDK.

2. Execute o comando PowerShell `New-ProvSchemeHardwareUpdate` para agendar uma Janela de Serviço para atualizações de hardware conforme especificado na versão do esquema de provisionamento.

Exemplo: `AllVMs` (novas e existentes) no catálogo de máquinas são consideradas para a atualização:

```
New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 4
-MaintenanceCycleDescription "Updating RAM and CPU Count to 8GB and 4"
-StartsNow -MaxDurationInMinutes 100 -ProvisioningSchemeName CVC
-PurgeDBAfterInDays 1 -SessionWarningTimeInMinutes 15
-SessionWarningLogOffTitle "Scheduled Maintenance"
-SessionWarningLogOffMessage "There is a scheduled maintenance coming up
and involves turning off the machine, please save your work and log out,
Thank You" -AllVMs
```

Exemplo: `NewVMsOnly` (novos e existentes) no catálogo de máquinas são considerados para a atualização:

```
New-ProvSchemeHardwareUpdate -ProvisioningSchemeVersion 4
-MaintenanceCycleDescription "Updating RAM and CPU Count to 8GB and 4"
-StartsNow -MaxDurationInMinutes 100 -ProvisioningSchemeName CVC
-PurgeDBAfterInDays 1 -SessionWarningTimeInMinutes 15
-SessionWarningLogOffTitle "Scheduled Maintenance"
-SessionWarningLogOffMessage "There is a scheduled maintenance coming up
and involves turning off the machine, please save your work and log out,
Thank You" -NewVMsOnly
```

Execute `Get-ProvSchemeHardwareUpdate` para recuperar objetos de Janela de Serviço associados a atualizações de esquema de hardware. Exemplo:

```
Get-ProvSchemeHardwareUpdate -MaintenanceCycleId xxxx-xxxx-yyyy-zzzz
```

Agendar atualizações de hardware em VMs específicas

1. Execute `New-ProvVmConfiguration` para criar uma nova configuração de VM de provisionamento. Para obter mais informações, consulte a documentação do SDK.
2. Execute o comando PowerShell `New-ProvVmHardwareUpdate` para agendar uma Janela de Serviço para atualizações de hardware conforme especificado na versão da configuração da VM.

Nota:

Para cada VM, quaisquer configurações personalizadas (versão da configuração da VM) sempre têm precedência sobre as especificações definidas na versão do esquema de provisionamento. Se uma configuração específica não for personalizada na VM, seu valor será herdado da versão do esquema de provisionamento associado.

Exemplo:

```
New-ProvVmHardwareUpdate -ProvVmConfigurationVersion 4 -StartsNow
-MaxDurationInMinutes 100 -ProvisioningSchemeName CVC -VMName AbcTest01
```

Execute `Get-ProvVmHardwareUpdate` para recuperar objetos de Janela de Serviço associados a atualizações de VM de hardware. Exemplo:

```
Get-ProvVmHardwareUpdate -MaintenanceCycleId xxxx-xxxx-yyyy-zzzz
```

Você também pode remover uma personalização usada para criar versões de VM de provisionamento usando o comando `Remove-ProvVmConfiguration`. Exemplo:

```
Remove-ProvVmConfiguration -Version 2 -VMName AbcTest01
```

Comandos PowerShell diversos associados à Janela de Serviço

- `Get-ProvMaintenanceCycle`: Recupera informações de todas as Janelas de Serviço. Exemplo:

  ```
  Get-ProvMaintenanceCycle -MaintenanceCycleId
  10073b8e-7e94-4527-8580-0e448eae0ad1
  ```

- `Get-ProvMaintenanceCycleVM`: Recupera informações de cada operação da Janela de Serviço para VMs individuais, juntamente com seu status. Exemplo:

  ```
  Get-ProvMaintenanceCycleVM -MaintenanceOperation HardwareUpdate
  -VirtualMachineSid 42263076-44ae-1ff9-f58b-62d57ddf8db5
  ```

Os vários status da Janela de Serviço são:

- Em execução
- Falhou
- Concluído
- Cancelando
- Cancelado
- NãoProcessado
- Pendente
- Incompleto
- Reparado
- Recuperando

- `Remove-ProvMaintenanceCycle`: Remove uma Janela de Serviço quando a Janela de Serviço não está ativa. Exemplo:

```
Remove-ProvMaintenanceCycle -MaintenanceCycleId
867af1ba-5b72-402e-9dc3-033298248f8e
```

- `Cancel-ProvMaintenanceCycle`: Se a operação ainda não foi iniciada pelo MCS em uma VM, este comando PowerShell cancela a operação. O MCS não cancela uma operação que está atualmente em execução na VM. Exemplo:

```
Cancel-ProvMaintenanceCycle -MaintenanceCycleId
867af1ba-5b72-402e-9dc3-033298248f8e
```

- `Restart-ProvMaintenanceCycle`: Se uma Janela de Serviço falhou ou está incompleta devido a causas externas, como o hipervisor estar inativo ou tempo insuficiente, este comando ajuda a reiniciar o ciclo e processar quaisquer trabalhos falhos ou não processados. Exemplo:

```
Restart-ProvMaintenanceCycle -MaintenanceCycleId
4f363b78-458a-403a-82e5-7fcc6caa498b -ScheduledStartTimeInUTC "June
19th 2024, 6AM" -MaxAllocatedDurationInMinutes 400
```

- `Update-ProvMaintenanceCycle`: Se uma Janela de Serviço já está agendada e não foi iniciada, este comando altera certos parâmetros.

Exemplo: Atualizar duração máxima:

```
Update-ProvMaintenanceCycle -MaintenanceCycleId
4f363b78-458a-403a-82e5-7fcc6caa498b -MaxDurationInMinutes 100
```

Exemplo: Atualizar VMs para um esquema de provisionamento:

```
Update-ProvMaintenanceCycle -MaintenanceCycleId
4f363b78-458a-403a-82e5-7fcc6caa498b -ProvisioningSchemeUid
867af1ba-5b72-402e-9dc3-033298248f8e -VMName ncn01,ncn02
```

Balancear carga de máquinas

O balanceamento de carga ajuda as organizações a alcançar o equilíbrio de custos desejado, ao mesmo tempo em que aproveitam tudo o que a nuvem tem a oferecer. O balanceamento de carga é configurado no nível do grupo de entrega.

> **Nota:**
>
> O balanceamento de carga se aplica apenas a máquinas de SO multi-sessão.
>
> O balanceamento de carga tem duas opções:

- Balanceamento de carga horizontal
- Balanceamento de carga vertical

Por padrão, o balanceamento de carga horizontal está ativado.

Balanceamento de carga horizontal: No modelo de balanceamento de carga horizontal, a sessão de usuário de entrada é atribuída à máquina menos carregada disponível. Considere este exemplo: em uma implantação, vamos supor que temos dois VDAs. Um tem uma sessão de usuário ativa (Usuário 1), e o segundo usuário (Usuário 2) está esperando por uma sessão. O algoritmo de balanceamento de carga horizontal atribui o Usuário 2 ao VDA 2 devido ao índice de carga mais favorável. Assim, o algoritmo horizontal distribui as sessões por todos os VDAs disponíveis, o que pode impedir que as máquinas sejam desligadas quando a carga diminui.

Balanceamento de carga vertical: No modelo de balanceamento de carga vertical, as sessões são atribuídas aos VDAs com o maior índice de carga. Isso ajuda a consolidar as sessões de

usuário de entrada em VDAs que já estão sendo usados por outros usuários e ajuda a reduzir o número de VDAs que devem ser ligados e mantidos prontos para sessões de usuário. Vamos considerar a mesma implantação mencionada no balanceamento de carga horizontal. O Usuário 1 é atribuído ao VDA 1, e o algoritmo de balanceamento de carga vertical é aplicado à sessão do Usuário 2. O Usuário 2 é atribuído ao VDA 1 porque o índice de carga mais alto está no VDA 1. Portanto, todas as sessões de entrada são atribuídas ao VDA mais carregado até que o limite máximo do índice de carga seja atingido. Somente então, o outro VDA começa a receber sessões.

Configuração de balanceamento de carga no nível do site

Você pode configurar o balanceamento de carga para todos os grupos de entrega (configuração em todo o site).

Para configurar este recurso no Studio, selecione **Configurações** no painel esquerdo e a guia **Configurações do site**. Selecione uma opção em **Balanceamento de Carga de Sessões em Máquinas**.

Alternativamente, você pode usar o PowerShell para habilitar ou desabilitar o balanceamento de carga vertical em todo o site. Use a configuração `UseVerticalScalingForRdsLaunches` no cmdlet `Set-BrokerSite`. Use `Get-BrokerSite` para exibir o valor da configuração `UseVerticalScalingForRdsLaunches`. Consulte a ajuda do cmdlet para obter detalhes.

> **Dica:**

> Para especificar o número máximo de sessões que uma máquina pode hospedar, use a configuração de política Número máximo de sessões.

Configuração de balanceamento de carga no nível do grupo de entrega

Você pode configurar o balanceamento de carga no nível do grupo de entrega e substituir a configuração de balanceamento de carga herdada do nível do site.

Você pode configurar isso durante a criação de um grupo de entrega ou a edição de um grupo de entrega existente. Consulte Etapa 2. Balanceamento de carga.

Gerenciamento de carga

O gerenciamento de carga mede a carga do servidor e determina qual servidor selecionar sob as condições ambientais atuais. Essa seleção é baseada em:

- **Status do modo de manutenção do servidor**: Uma máquina de SO multi-sessão é considerada para balanceamento de carga somente quando o modo de manutenção está desativado.
- **Índice de carga do servidor**: Determina a probabilidade de um servidor que entrega máquinas de SO multi-sessão receber conexões. O índice é uma combinação de avaliadores de carga: o número de sessões e as configurações para métricas de desempenho, como uso de CPU, disco e memória. Os avaliadores de carga são especificados nas configurações da política de gerenciamento de carga. Por padrão, o índice de carga usa apenas o número de sessões em seu cálculo, e não CPU, disco ou memória, até que sejam configurados nas configurações da política de gerenciamento de carga. Para obter informações sobre as configurações da política, consulte Configurações da política de gerenciamento de carga.

  Um índice de carga do servidor de 10000 indica que o servidor está totalmente carregado. Se nenhum outro servidor estiver disponível, os usuários poderão receber uma mensagem de que a área de trabalho ou o aplicativo está indisponível no momento ao iniciar uma sessão. Você pode monitorar o índice de carga no Director (Monitor), em uma pesquisa do Studio e no SDK.

  Nas exibições do console, para exibir a coluna **Índice de Carga do Servidor** (que está oculta por padrão), selecione uma máquina, clique com o botão direito do mouse em um cabeçalho de coluna e selecione **Selecionar Coluna**. Na **categoria Máquina**, selecione **Índice de Carga**.

  No SDK, use o cmdlet `Get-BrokerMachine`. Para obter detalhes, consulte CTX202150.
- **Configuração da política de tolerância de logon simultâneo**: O número máximo de solicitações simultâneas para fazer logon no servidor. (Essa configuração é equivalente à limitação de carga nas versões do XenApp 6.x.)

  Quando todos os servidores estão no nível ou acima da configuração de tolerância de logon simultâneo, a próxima solicitação de logon é atribuída ao servidor com o menor número de logons pendentes. Se mais de um servidor atender a esses critérios, o servidor com o menor índice de carga será selecionado. Consulte Tolerância de logon simultâneo.

  > **Dica:**
  >
  > Para aplicar a configuração de tolerância de logon e fazer com que os logons simultâneos que excedem o número especificado falhem, você pode executar `Set-BrokerServiceConfigurationData Core.LogonToleranceIsHardLimit -SettingValue $true`.

Criar grupos de entrega

Introdução

Um grupo de entrega é uma coleção de máquinas escolhidas de um ou mais catálogos de máquinas. Os grupos de entrega definem quais usuários podem acessar essas máquinas e os aplicativos e desktops disponíveis para eles.

Criar um grupo de entrega é o próximo passo após configurar seu site e catálogos de máquinas. Você pode modificar as configurações iniciais posteriormente ou criar grupos de entrega adicionais conforme necessário.

Alguns recursos e configurações são configuráveis apenas ao editar um grupo de entrega existente. Para obter mais detalhes, consulte Gerenciar grupos de entrega.

Antes de começar

Antes de criar um grupo de entrega:

- Revise este artigo para entender as escolhas e informações necessárias.
- Certifique-se de ter criado uma conexão com o hipervisor, serviço de nuvem ou outro recurso que hospeda suas máquinas.
- Certifique-se de que um catálogo de máquinas com máquinas virtuais ou físicas esteja disponível.

Páginas do Assistente

Se você criou um site e um catálogo de máquinas, mas não um grupo de entrega, o Web Studio o guiará para o ponto de partida correto para criar um.

Se você já criou um grupo de entrega e deseja criar outro, siga estas etapas:

1. Selecione **Grupos de entrega**.
2. No painel de ações, selecione **Criar Grupo de Entrega**.
3. Para organizar grupos de entrega, você pode criar pastas sob a pasta padrão **Delivery Groups**. Para obter mais informações, consulte Criar uma pasta.
4. Selecione a pasta onde você deseja criar o grupo e clique em **Create Delivery Group**. O assistente de criação de grupo é aberto.

5. O assistente começa com uma página de **Introdução**, que você pode optar por pular em lançamentos futuros. Em seguida, ele o guia por várias páginas, conforme descrito na tabela a seguir. Após concluir cada página, clique em **Next** para prosseguir até chegar à página final.

	SO MULTISSESSÃO	SO DE SESSÃO ÚNICA ESTÁTICO (ATRIBUÍDO)	SO DE SESSÃO ÚNICA COMPARTILHADO (AGRUPADO)	ACESSO REMOTO AO PC
Páginas	Máquinas	Máquinas	Máquinas	Máquinas
	Balanceamento de Carga	Tipo de Entrega	Usuários	Usuários
	Usuários	Usuários	Aplicativos	Aplicativos
	Aplicativos	Aplicativos	Desktops	Regras de Atribuição de Desktop
	Desktops	Regras de Atribuição de Desktop	Proteção de Aplicativos	Proteção de Aplicativos
	Proteção de Aplicativos	Proteção de Aplicativos	Escopos	Escopos
	Escopos	Escopos	Contrato de licença	Contrato de licença
	Contrato de licença	Contrato de licença	Conjunto de Políticas	Conjunto de Políticas
	Conjunto de Políticas	Conjunto de Políticas	Cache de Host Local	Resumo
	Resumo	Resumo	Resumo	

Nota:

- Você vê a página **Alocação de Máquina** (logo após a página **Máquinas**) se houver alguma máquina atribuída disponível no catálogo de máquinas estáticas de SO de sessão única selecionado.
- A página do modo Cache de Host Local está disponível apenas para grupos de entrega que contêm máquinas agrupadas de sessão única gerenciadas por energia.

Página Máquinas

1. Para criar um grupo de entrega com VMs de sessão única com capacidade de suspensão, selecione **Exigir capacidade de suspensão para este grupo de entrega**.

   Nota:

   Este recurso é aplicável apenas a máquinas de sessão única com capacidade de suspensão.

2. Selecione um catálogo de máquinas e selecione o número de máquinas que você deseja usar desse catálogo.

Considerações importantes

- Ao escolher um catálogo, a lista mostra apenas catálogos com pelo menos uma máquina não utilizada.
- Um catálogo pode fornecer máquinas para mais de um grupo de entrega. Uma máquina pode ser usada em apenas um grupo de entrega. Quando você adiciona mais máquinas ao grupo de entrega, o Web Studio sugere o mesmo catálogo por padrão.
- Um grupo de entrega pode usar máquinas de mais de um catálogo; no entanto, esses catálogos devem conter os mesmos tipos de máquina (SO multissessão, SO de sessão única ou Acesso Remoto para PC). Todas as máquinas dentro de um grupo de entrega devem ter o mesmo tipo de atribuição (agrupado ou estático). Em outras palavras, você não pode misturar tipos de máquina em um grupo de entrega.
- A Citrix® recomenda usar a versão mais recente do VDA em todas as máquinas.
- Para **Acesso Remoto para PC**, quando você cria um site, um catálogo chamado **Máquinas de Acesso Remoto para PC** e um grupo de entrega chamado **Desktops de Acesso Remoto para PC** são criados automaticamente. Cada máquina em um catálogo de **Máquinas de Acesso Remoto para PC** é automaticamente associada a um grupo de entrega.

- As seguintes verificações de compatibilidade são realizadas:
  - MinimumFunctionalLevel deve ser compatível
  - SessionSupport deve ser compatível
  - AllocationType deve ser compatível para SingleSession
  - Acesso Remoto para PC é compatível apenas com o catálogo de Acesso Remoto para PC

Página de Alocação de Máquinas

A página **Alocação de Máquinas** está disponível se houver alguma máquina atribuída disponível no catálogo de máquinas estáticas de SO de sessão única selecionado na página **Máquinas**.

Usando esta página, gerencie as atribuições de usuário e os nomes de exibição da área de trabalho para as máquinas neste grupo de entrega.

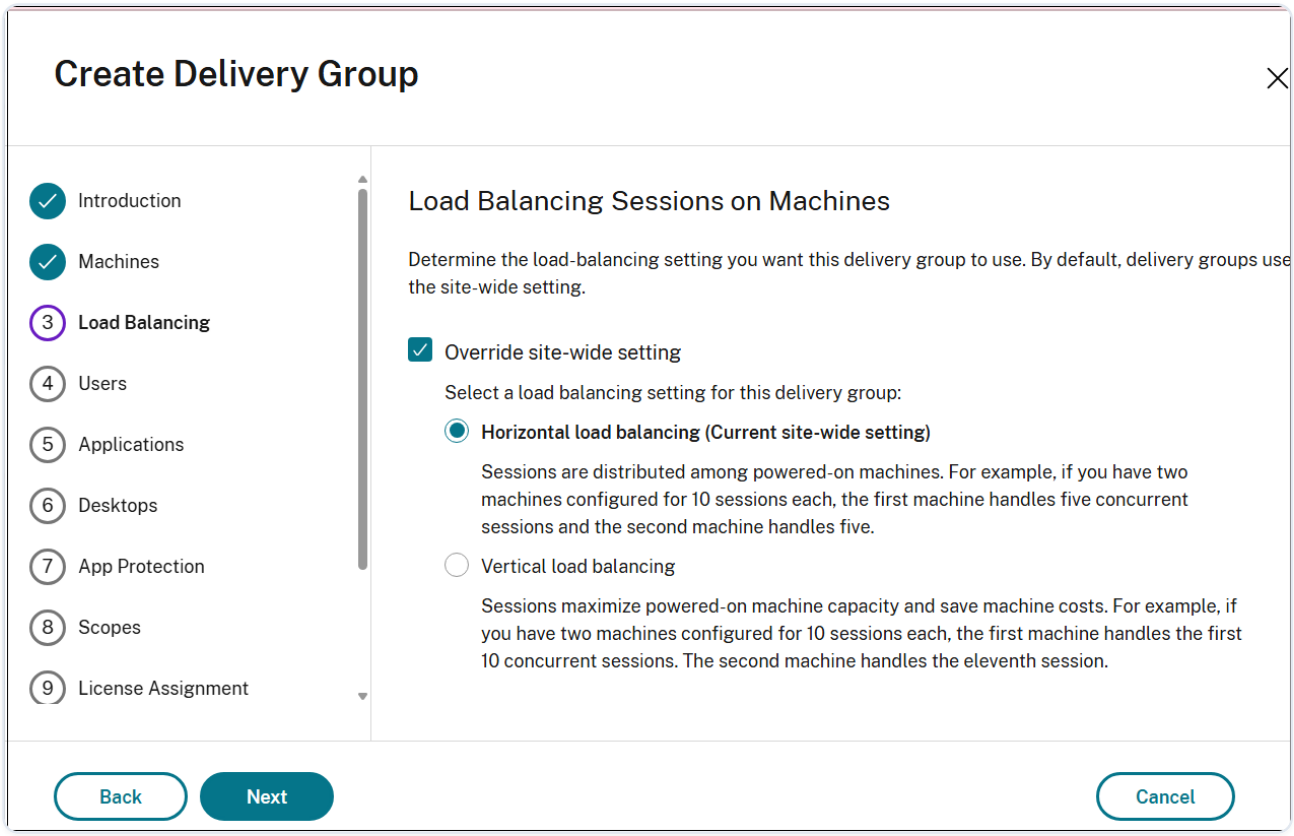
- Use o campo **Nome de exibição** para gerenciar o nome de exibição da área de trabalho.
- Clique em **Procurar** e selecione usuários ou grupos.

Página de Balanceamento de Carga

A página **Balanceamento de Carga de Sessões em Máquinas** está disponível para máquinas de SO multi-sessão.

Usando esta página, configure a definição de balanceamento de carga que você deseja que este grupo de entrega use. Por padrão, os grupos de entrega usam a definição de todo o site.

1. Para configurar uma definição de balanceamento de carga para este grupo de entrega, selecione a caixa de seleção **Substituir definição de todo o site**.
2. Selecione a opção **Balanceamento de carga horizontal** ou **Balanceamento de carga vertical**, conforme necessário. Para obter informações sobre os métodos de balanceamento de carga horizontal e vertical, consulte Balancear máquinas.



Se você selecionar **Balanceamento de carga vertical**, certifique-se de que as políticas Tolerância de logon simultâneo e Número máximo de sessões estejam configuradas adequadamente.

Página Tipo de Entrega

A página **Tipo de Entrega** aparece apenas para máquinas estáticas (atribuídas) de SO de sessão única.

Usando esta página, configure as máquinas no catálogo para entregar desktops ou aplicativos aos seus usuários.

1. Selecione **Aplicativos** ou **Desktops.** Você não pode habilitar ambos.

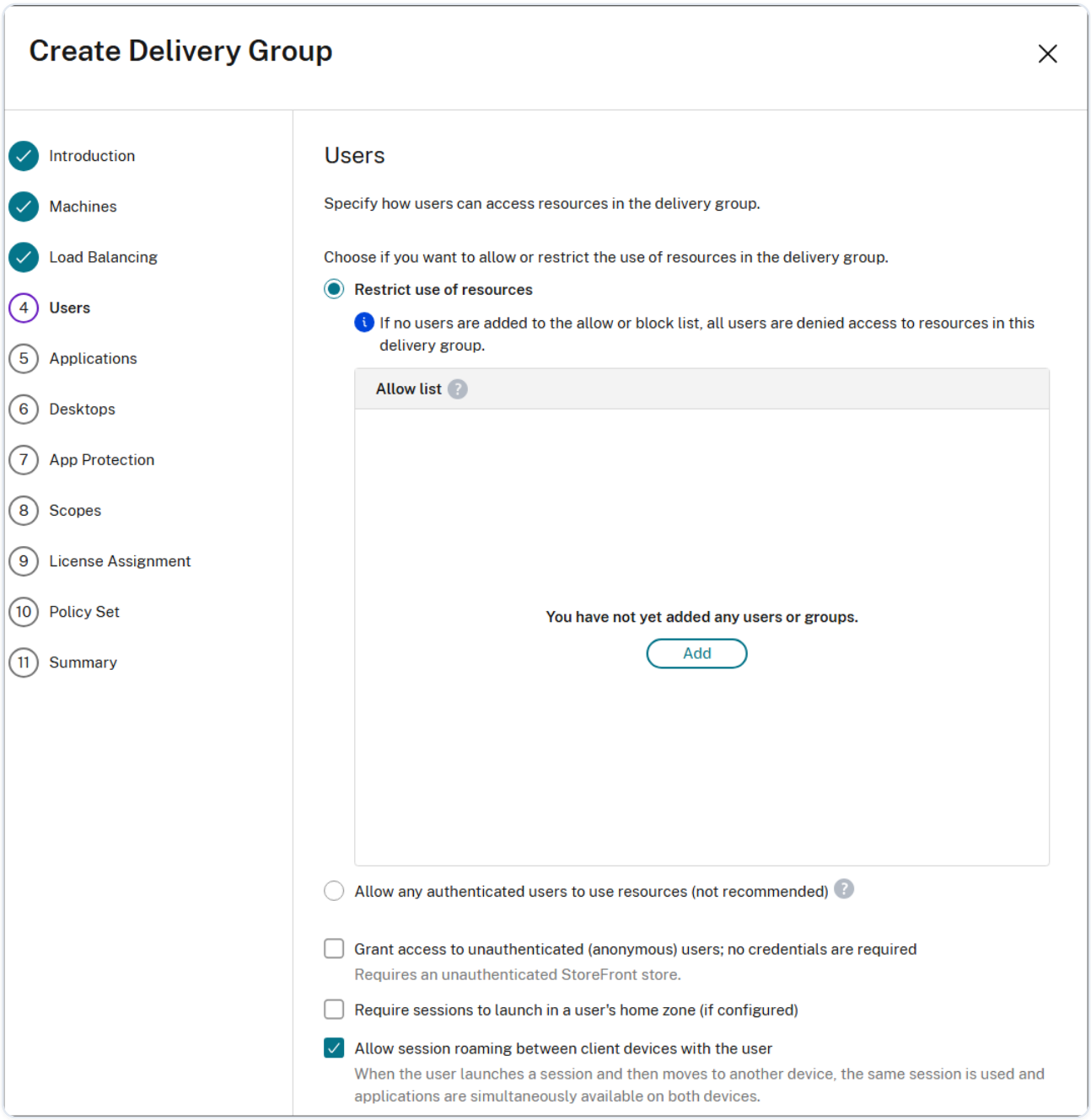
> **Nota:**
>
> Se você selecionar máquinas de um catálogo de SO multi-sessão ou SO de sessão única aleatório (agrupado), o tipo de entrega é assumido como aplicativos e desktops. Você pode entregar aplicativos, desktops ou ambos.

Página Usuários

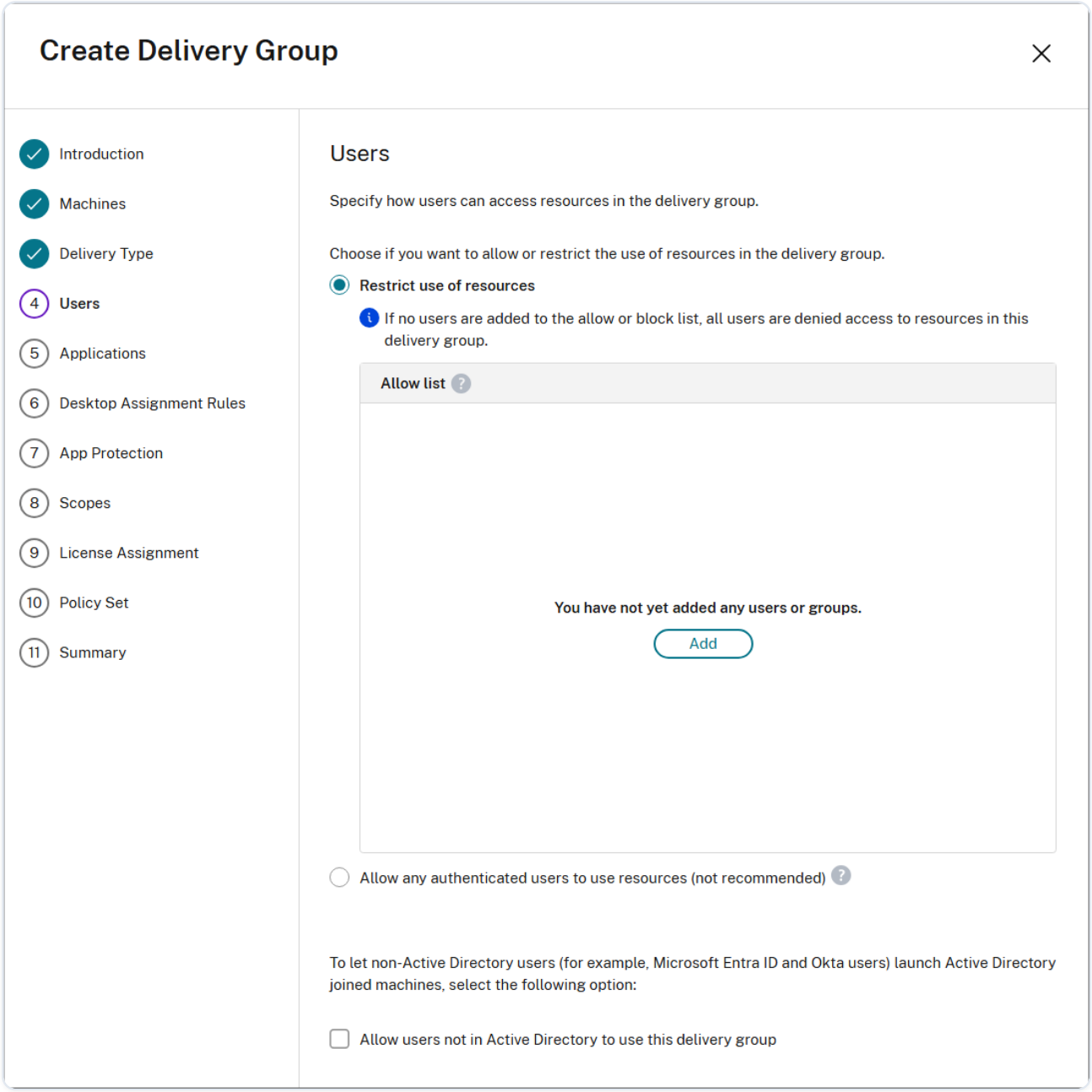
A página **Usuários** está disponível para todos os tipos de máquina. No entanto, as opções da página variam com diferentes tipos de máquinas.

Usando esta página, especifique como os usuários podem acessar recursos no grupo de entrega.

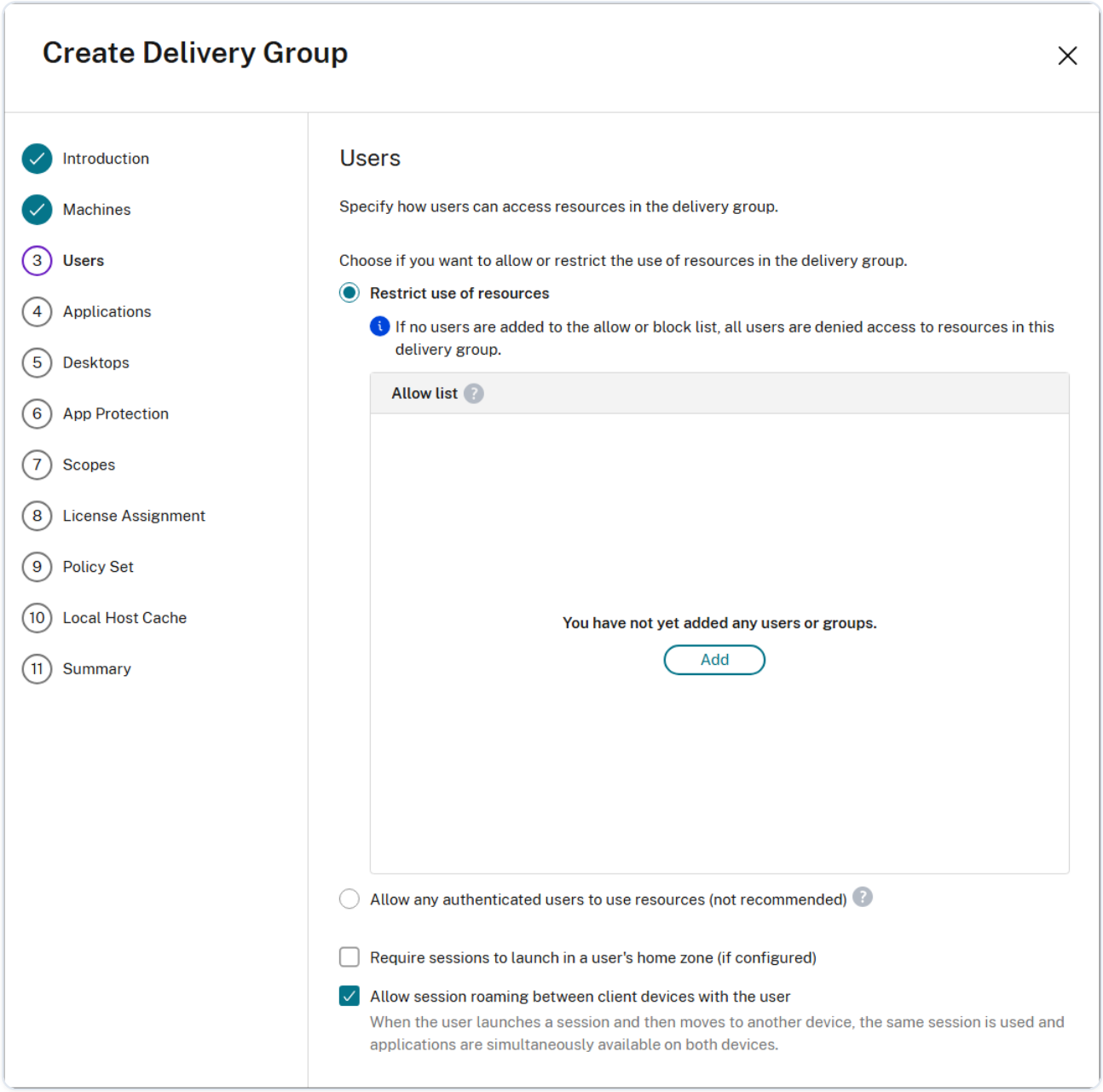
Para máquinas de SO multi-sessão:



Para máquinas de SO de sessão única estáticas:



Para máquinas de SO de sessão única compartilhadas:



Como funciona o controle de acesso do usuário

O acesso do usuário em um grupo de entrega é controlado por meio de listas de usuários especificadas ao criar ou editar as configurações de acesso.

- Usuários que atendem a *todas* as seguintes condições podem acessar **aplicativos** em um grupo de entrega:
  - Têm acesso a recursos (aplicativos e desktops) neste grupo de entrega. Por padrão, o acesso é determinado pela lista de acesso de usuários da implantação (usuários no Active Directory), que não é configurada via Studio. Consulte Adicionar ou remover usuários em um grupo de entrega.

  - Têm acesso a aplicativos neste grupo. Por padrão, a regra de política de direito de aplicativo inclui todos. Consulte os cmdlets `BrokerAppEntitlementPolicyRule` do SDK do PowerShell para obter detalhes. Se necessário, você pode restringir o acesso do usuário a aplicativos em um grupo de entrega usando **Grupos de Entrega > Editar Regra de Atribuição de Aplicativo**.
  - Têm acesso a grupos de aplicativos que incluem este aplicativo.

- Usuários que atendem a *ambas* as seguintes condições podem acessar desktops em um grupo de entrega:

  - Têm acesso a recursos (aplicativos e desktops) neste grupo de entrega. Por padrão, o acesso é determinado pela lista de acesso de usuários da implantação (usuários no Active Directory), que não é configurada via Studio. Você pode adicionar ou remover usuários do escopo de usuário padrão. Consulte Adicionar ou remover usuários em um grupo de entrega.
  - Têm acesso a desktops neste grupo. Para obter mais informações, consulte Desktops (ou página Regras de Atribuição de Desktop).

> **Nota:**

> - Ao especificar uma lista de usuários ou grupos, você pode selecionar contas de qualquer tipo de identidade conectado, incluindo Active Directory, Microsoft Entra ID ou Okta. Além disso, você pode selecionar contas de vários provedores do mesmo tipo de identidade.

Etapas de configuração

1. Selecione uma das opções para permitir ou restringir o uso de recursos no grupo de entrega.

   - **Permitir que quaisquer usuários autenticados usem recursos:** Para acessar aplicativos e desktops, os usuários e membros do grupo que você especificar pelo nome devem apresentar credenciais como cartão inteligente ou nome de usuário e senha para o StoreFront™ ou o aplicativo Citrix Workspace™. (Para grupos de entrega que contêm máquinas de SO de sessão única, você pode importar dados de usuário (uma lista de usuários) posteriormente, editando o grupo de entrega.)
   - **Restringir o uso de recursos:** Alternativamente, você pode restringir o uso de um grupo de entrega adicionando usuários ou grupos de usuários à **Lista de permissões**. Somente usuários na **Lista de permissões** podem acessar aplicativos e desktops no grupo de

entrega. Você também pode adicionar usuários e grupos de usuários a uma lista de bloqueio clicando em **Adicionar lista de bloqueio**, o que impede que os usuários usem aplicativos e desktops no grupo de entrega selecionado. Uma lista de bloqueio só é significativa quando usada para bloquear usuários na lista de permissões.

2. Para máquinas de SO de várias sessões, selecione **Conceder acesso a usuários não autenticados (anônimos); nenhuma credencial é necessária** se você quiser que os usuários acessem aplicativos e desktops sem apresentar credenciais ao StoreFront ou ao aplicativo Citrix Workspace. Por exemplo, em quiosques, o aplicativo pode exigir credenciais, mas o portal de acesso e as ferramentas do Citrix não.

   - Contas de usuário não autenticadas são criadas sob demanda quando uma sessão é iniciada e nomeadas AnonXYZ, onde XYZ é um valor exclusivo de três dígitos.
   - Sessões de usuário não autenticadas têm um tempo limite de inatividade padrão de 10 minutos e são desconectadas automaticamente quando o cliente se desconecta. Reconexão, roaming entre clientes e Workspace Control não são suportados.

3. Selecione **Exigir que as sessões sejam iniciadas na zona inicial de um usuário (se configurado**) para evitar que as sessões sejam padronizadas para outras zonas disponíveis se a zona inicial do usuário tiver recursos suficientes.
4. Selecione **Permitir roaming de sessão entre dispositivos cliente com o usuário** se você quiser que as sessões sigam, independentemente do dispositivo ou se as sessões atuais existirem. Consulte Roaming de sessão.
5. Para permitir que usuários não-Active Directory iniciem sessões em máquinas usando uma conta local, selecione a caixa de seleção **Permitir que usuários não no Active Directory usem este grupo de entrega**. Esta ação facilita a criação e o mapeamento automático de uma conta local do Windows para o usuário logado. Consequentemente, todos os logins para este grupo de entrega usarão uma conta local mapeada nos VDAs para login. Embora permitir que usuários não-Active Directory acessem uma conta local no VDA seja um caso de uso, essa funcionalidade também se estende aos logins do Active Directory.

> **Nota:**
>
> Se o UPN do Azure do usuário contiver um ponto como o vigésimo caractere, o VDA do Windows Server não conseguirá criar uma conta de usuário local.

A tabela a seguir descreve suas escolhas na página **Usuários**:

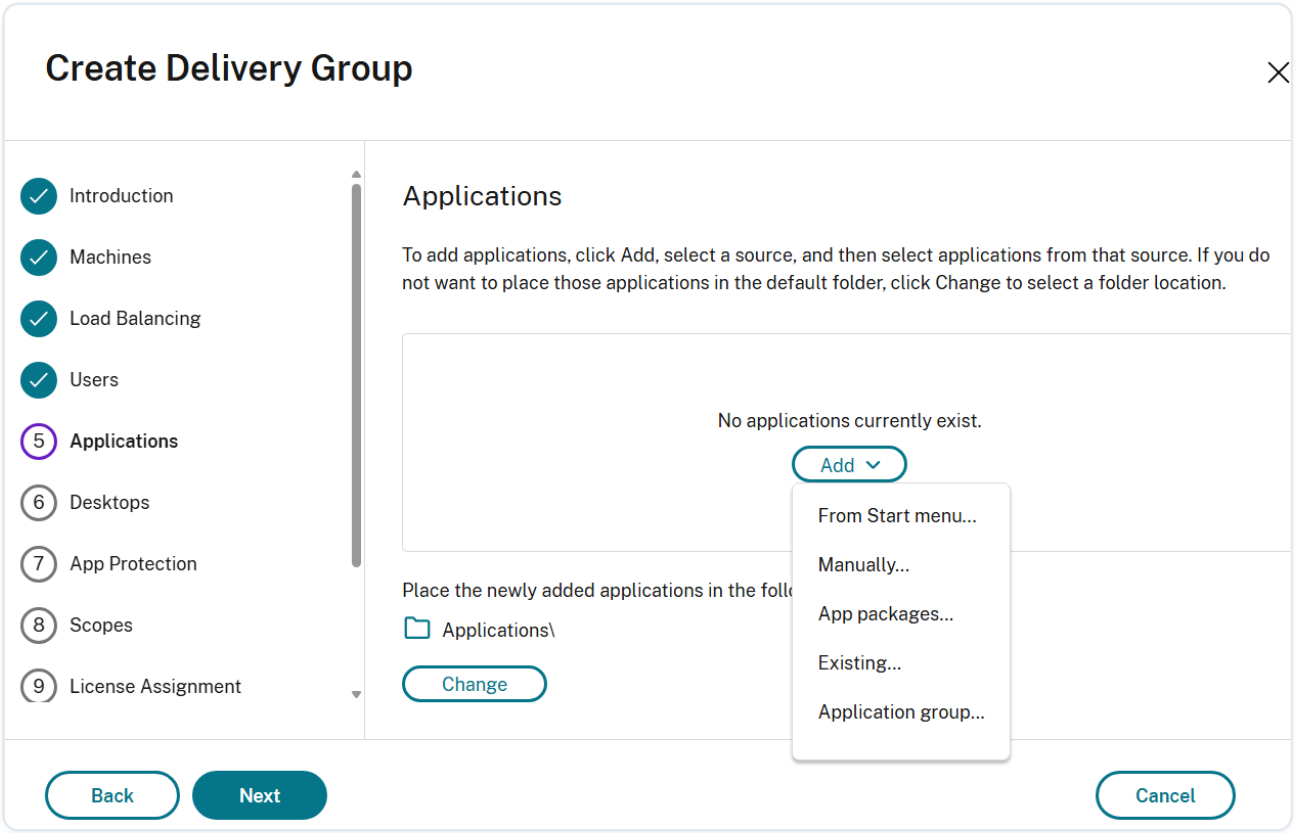
HABILITAR ACESSO PARA	ADICIONAR/ATRIBUIR USUÁRIOS E GRUPOS DE USUÁRIOS?	HABILITAR A CAIXA DE SELEÇÃO “CONCEDER ACESSO A USUÁRIOS NÃO AUTENTICADOS”?
Apenas usuários autenticados	Sim	Não
Apenas usuários não autenticados	Não	Sim
Usuários autenticados e não autenticados	Sim	Sim

Página Aplicativos

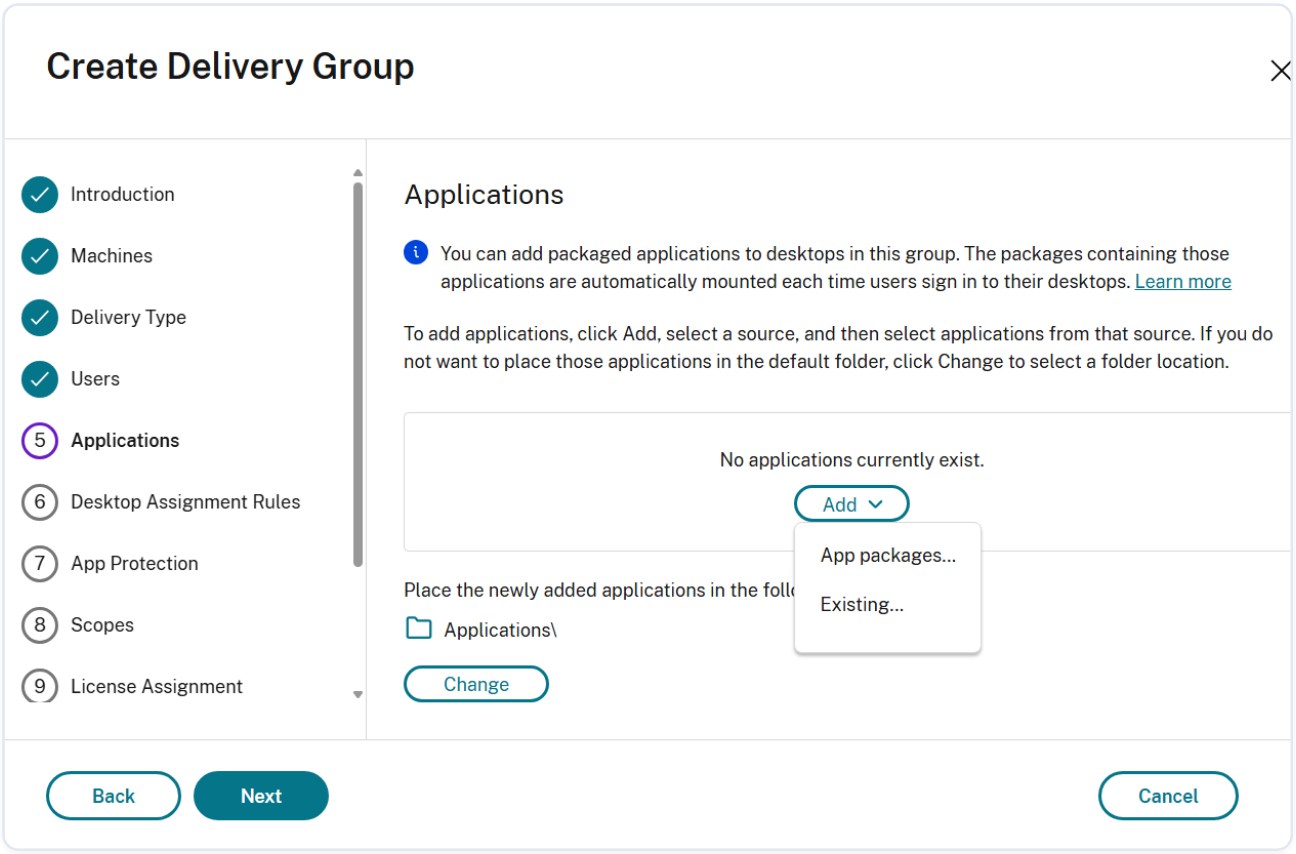
A página **Aplicativos** está disponível para todos os tipos de máquina. No entanto, os aplicativos que você pode adicionar variam de acordo com os diferentes tipos de máquinas.

Usando esta página, você pode adicionar aplicativos empacotados a desktops neste grupo.

Para máquinas de SO compartilhadas de sessão múltipla e sessão única:



Para máquinas de SO estáticas de sessão única:



Considerações importantes

- Você pode adicionar aplicativos empacotados a grupos de entrega. Os pacotes que contêm esses aplicativos são montados automaticamente cada vez que os usuários fazem logon em seus desktops ou PCs remotos.
- Por padrão, os novos aplicativos que você adiciona são colocados em uma pasta chamada Aplicativos. Você pode especificar uma pasta diferente. Para obter detalhes, consulte o artigo Aplicativos.
- Você pode alterar as propriedades de um aplicativo ao adicioná-lo a um grupo de entrega, ou posteriormente. Para obter detalhes, consulte o artigo Aplicativos.
- Se você tentar adicionar um aplicativo e já existir um com o mesmo nome nessa pasta, será solicitado que você renomeie o aplicativo que está adicionando. Se você recusar, o aplicativo será adicionado com um sufixo que o torna exclusivo dentro dessa pasta de aplicativo.
- Ao adicionar um aplicativo a mais de um grupo de entrega, um problema de visibilidade pode ocorrer se você não tiver permissão para visualizar o aplicativo em todos esses grupos de entrega. Nesses casos, consulte um administrador com permissões maiores ou solicite que seu escopo seja estendido para incluir todos os grupos de entrega aos quais o aplicativo foi adicionado.

- Se você publicar dois aplicativos com o mesmo nome para os mesmos usuários, altere a propriedade Nome do aplicativo (para usuário). Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.

Etapas de configuração

1. Selecione o menu **Adicionar** para exibir as fontes do aplicativo.

    - **Do menu Iniciar:** Os aplicativos são descobertos por meio de um dos VDAs atualmente registrados que são atribuídos ao grupo de entrega. Ao selecionar esta fonte, uma nova página é aberta com uma lista de aplicativos descobertos; selecione os que deseja adicionar e, em seguida, selecione **OK**.
    - **Manualmente:** Aplicativos localizados na implantação ou em outro lugar da sua rede. Ao selecionar esta fonte, uma nova página é aberta onde você digita o caminho para o executável, o diretório de trabalho, os argumentos opcionais da linha de comando e os nomes de exibição para administradores e usuários. Depois de inserir essas informações, selecione **OK**.
    - **Existente:** Aplicativos adicionados anteriormente à implantação, talvez em outro grupo de entrega. Ao selecionar esta fonte, uma nova página é aberta com uma lista de aplicativos descobertos; selecione os que deseja adicionar e, em seguida, selecione **OK**.
    - **Pacotes de aplicativos:** Aplicativos em pacotes de aplicativos App-V, MSIX, MSIX app attach ou FlexApp. Ao selecionar esta fonte, a página **Adicionar Aplicativos de Pacotes** é aberta. Selecione uma fonte de pacote de aplicativos, selecione os aplicativos que deseja adicionar na exibição resultante e, em seguida, selecione **OK**.

        > **Nota:**
        >
        > ◦ Esta opção fica esmaecida se nenhum pacote de aplicativo estiver configurado para o site.
        >
        > \> - Para publicar aplicativos MSIX ou MSIX app attach, o nível funcional do grupo de entrega deve ser 2106 ou posterior. Para aplicativos FlexApp, o nível funcional deve ser 2206 ou posterior. Quando um requisito de nível funcional não é atendido, as opções correspondentes na lista suspensa **Fonte do pacote de aplicativos** ficam esmaecidas.

- **Grupo de aplicativos:** Grupos de aplicativos que existem na implantação.

Se uma fonte de aplicativo ou aplicativo não estiver disponível ou for inválido, ele não estará visível ou não poderá ser selecionado. Por exemplo, a fonte **Existente** não está disponível se nenhum aplicativo tiver sido adicionado à implantação. Ou, um aplicativo pode não ser compatível com os tipos de sessão suportados em máquinas no catálogo de máquinas selecionado.

Página de Desktops (ou Regras de Atribuição de Desktop)

O título desta página depende do catálogo de máquinas que você escolheu anteriormente no assistente:

- Se você escolher um catálogo contendo máquinas de sessão única multi-sessão ou agrupadas, esta página será intitulada **Desktops**.
- Se você escolher um catálogo contendo máquinas estáticas de sessão única e especificou “Desktops” na página **Tipo de Entrega**, esta página será intitulada **Regras de Atribuição de Desktop**.

> **Nota:**
>
> - Se você escolher um catálogo contendo máquinas estáticas de sessão única e especificou “Aplicativos” na página **Tipo de Entrega**, então você não verá a página.

1. (Opcional) Para atualizar o ícone de desktop padrão para o grupo de entrega, selecione **Alterar**. Você pode extrair o ícone de um arquivo `.ico` ou de um arquivo `.exe`. O tamanho máximo de arquivo de ícone suportado é de 500 KB. Este ícone se aplica a todos os desktops no grupo, a menos que um ícone diferente seja definido para um desktop individual.
2. Selecione **Adicionar**. Na caixa de diálogo:
    a. Nos campos **Nome de exibição** e **Descrição**, digite as informações a serem exibidas no aplicativo Citrix Workspace.
    b. Para máquinas OS de sessão única multi-sessão ou agrupadas: Para adicionar uma restrição de tag a um desktop, selecione **Restringir inicializações a máquinas com esta tag** e, em seguida, selecione a tag no menu.
    c. Usando os botões de opção, você pode:
        i. **Permitir que todos com acesso a este grupo de entrega usem um desktop.** Todos os usuários no grupo de entrega podem iniciar um desktop (para grupos com máquinas

agrupadas) ou ter uma máquina atribuída quando iniciam o desktop (para grupos com máquinas estáticas de sessão única).

ii. **Restringir o uso do desktop** adicionando usuários e grupos de usuários à **Lista de permissões**. Somente os usuários na **Lista de permissões** podem acessar um desktop. Você também pode adicionar usuários e grupos de usuários a uma lista de bloqueio clicando em **Adicionar lista de bloqueio**, o que impede que os usuários usem desktops no grupo de entrega selecionado. Uma lista de bloqueio só é significativa quando usada para bloquear usuários na lista de permissões.

d. Se o grupo contiver máquinas estáticas de sessão única, especifique o número máximo de desktops por usuário. Este deve ser um valor de um ou maior. A configuração não é obrigatória. Você pode atribuir máquinas manualmente ou usar o RemotePC para que as máquinas sejam atribuídas automaticamente.

e. (Opcional) Selecione **Alterar** para atualizar o ícone do desktop para desktops agrupados ou a regra de atribuição de desktop para desktops estáticos de sessão única. Você pode navegar para selecionar um ícone de um arquivo `.ico` ou de um arquivo `.exe`. O ícone especificado substitui o ícone padrão definido no nível do grupo de entrega.

f. Habilitar ou desabilitar o desktop (para máquinas multi-sessão) ou a regra de atribuição de desktop (para máquinas estáticas de sessão única): Desabilitar um desktop interrompe a entrega do desktop. Desabilitar uma regra de atribuição de desktop interrompe a atribuição automática de desktop aos usuários.

g. Quando terminar com a caixa de diálogo, selecione **OK**.

Página de Proteção de Aplicativos

A página **Proteção de Aplicativos** está disponível para todos os tipos de máquina.

Usando esta página, você fornece segurança aprimorada para aplicativos e desktops publicados do Citrix.

As informações a seguir são complementares ao artigo Proteção de aplicativos na documentação do Citrix Virtual Apps and Desktops. Para usar a proteção de aplicativos em uma implantação do Citrix DaaS, siga as orientações gerais desse artigo, observando os seguintes detalhes.

- Você deve ter uma assinatura válida do Citrix Cloud™ e direitos de proteção de aplicativos válidos. Para adquirir o recurso de proteção de aplicativos, você pode entrar em contato com seu representante de vendas da Citrix. (Para implantações locais: Você deve ter um direito de Proteção de Aplicativos válido. Para adquirir o recurso de Proteção de Aplicativos, entre em contato com seu representante de vendas da Citrix.)

- A proteção de aplicativos requer confiança XML. Para habilitar a confiança XML, vá para **Configurações > Configurações do site > Habilitar confiança XML**.

A proteção é aplicada nas seguintes condições:

- **Anti-captura de tela**:
  - No Windows e macOS, apenas a janela do conteúdo protegido fica em branco. A proteção de aplicativos está ativa quando uma janela protegida não está minimizada.
  - No Linux, a captura inteira fica em branco. A proteção de aplicativos está ativa independentemente de uma janela protegida estar minimizada ou não.
- **Anti-registro de teclas**: Habilitado se uma janela protegida estiver em foco. Para desabilitar a proteção, mude o foco para outra janela.

Página de Escopos

A página **Escopos** está disponível para todos os tipos de máquina.

Usando esta página, agrupe objetos (por exemplo, conexões, catálogos e grupos de entrega) de uma forma que seja relevante para sua organização.

Página de atribuição de licenças

A página **Atribuição de licença** está disponível para todos os tipos de máquina.

Usando esta página, especifique qual licença você deseja que o grupo de entrega use. Por padrão, o grupo de entrega usa a licença do site. Para obter mais informações, consulte Licenças.

Página Conjunto de Políticas

A página **Conjunto de Políticas** está disponível para todos os tipos de máquina.

Usando esta página, especifique qual conjunto de políticas você deseja que este grupo de entrega use.

Página Modo de Cache do Host Local

Esta página está disponível apenas para grupos de entrega que contêm máquinas agrupadas de sessão única gerenciadas por energia.

Por padrão, as máquinas agrupadas gerenciadas por energia podem ser usadas para apenas uma sessão quando no modo Cache de Host Local (LHC). Para alterar o comportamento padrão e

torná-las sempre disponíveis para novas conexões de usuário quando no modo LHC, selecione **Usar máquinas para sessões subsequentes**.

Alternativamente, você pode alterar o comportamento padrão usando comandos PowerShell. Para obter mais informações, consulte Suporte a aplicativos e desktops.

> **Importante:**
>
> Habilitar o acesso a máquinas agrupadas de sessão única gerenciadas por energia pode fazer com que dados e alterações de sessões de usuário anteriores estejam presentes em sessões subsequentes.

Desktops agrupados de uso único no Cache de Host Local

Durante uma interrupção do Cache de Host Local (LHC), os desktops agrupados podem ser usados uma única vez. Isso é conseguido emitindo um blob de higiene para VDAs capazes e iniciando reinicializações. Este processo garante um estado limpo para os desktops após a recuperação da interrupção. Para máquinas que não são capazes ou legadas, a participação ocorre apenas se a reutilização for explicitamente habilitada. O recurso melhora a satisfação do cliente durante interrupções, tornando a disponibilidade mais contínua.

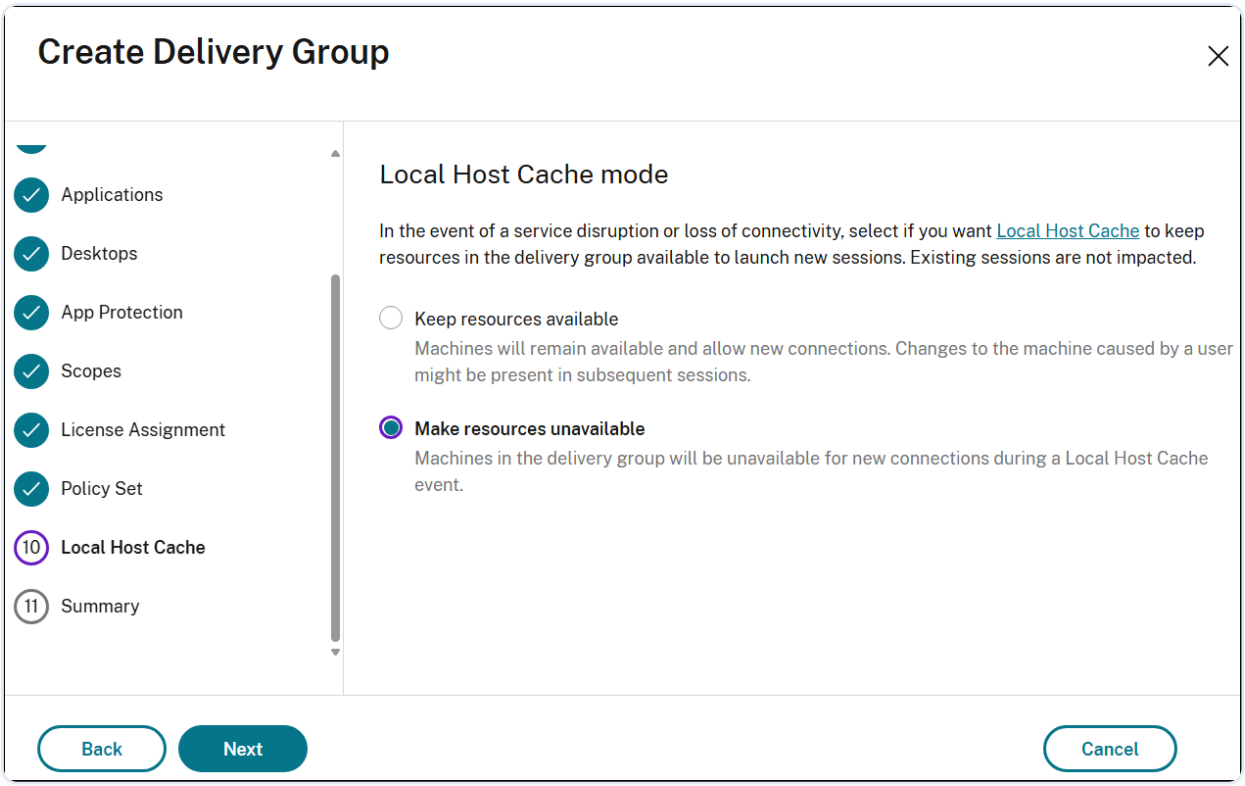
Pré-requisitos

- VDA versão 2407 ou posterior para aplicação total da higiene. VDAs legados (anteriores à versão 2407 do VDA) podem ser usados apenas quando a reutilização está habilitada. Esses VDAs não recebem o blob de higiene ou reinicializações forçadas.
- Catálogos de máquinas com máquinas de sessão única.

Configurar o uso único de desktops agrupados

1. Crie um catálogo MCS com máquinas de sessão única usando o VDA build 2407 ou superior.
2. Crie um grupo de entrega correspondente. Defina a configuração do grupo de desktop `ReuseMachinesWithoutShutdownInOutage` como `false` para o grupo de entrega a partir do Remote PowerShell ou selecione **Tornar recursos indisponíveis** no Studio na página **Modo de Cache de Host Local** ao criar um grupo de entrega.

```
Set-BrokerDesktopGroup -Name "name"
-ReuseMachinesWithoutShutdownInOutage $false
```



3. Após concluir a configuração, durante o modo de interrupção do LHC, as máquinas ficam disponíveis para uso único. Quando fora do modo de interrupção do LHC, as máquinas que foram 'contaminadas' são reiniciadas e ficam disponíveis para serem usadas novamente.

> **Nota:**
>
> Uma máquina é classificada como 'contaminada' assim que uma sessão de usuário é iniciada após sua última inicialização. Uma máquina 'não contaminada' refere-se a uma máquina que não iniciou nenhuma sessão de usuário desde seu último evento de inicialização.

Página de resumo

Insira um nome para o grupo de entrega. Você também pode (opcionalmente) inserir uma descrição, que aparece no aplicativo Citrix Workspace e no Studio.

Revise as informações de resumo e clique em **Concluir**.

Limitação

A atribuição de um desktop a um endereço IP de cliente funciona apenas com um conjunto limitado de tipos e configurações de cliente. A realização de filtragem de acesso com base no endereço IP do cliente usa o endereço IP público para clientes em nuvem.

Mais informações

- Gerenciar grupos de entrega
- Aplicativos

Gerenciar grupos de entrega

Introdução

Este artigo descreve os procedimentos para gerenciar grupos de entrega a partir do console de gerenciamento. Além de alterar as configurações especificadas ao criar o grupo, você pode configurar outras configurações que não estão disponíveis ao criar um grupo de entrega.

Os procedimentos são organizados de acordo com as categorias: geral, usuários, máquinas e sessões. Algumas tarefas abrangem mais de uma categoria. Por exemplo, "Impedir que usuários se conectem a máquinas" é descrito na categoria de máquinas, mas também afeta os usuários. Portanto, se você não conseguir encontrar uma tarefa em uma categoria, verifique uma categoria relacionada.

Outros artigos também contêm informações relacionadas:

- Aplicativos contêm informações sobre o gerenciamento de aplicativos em grupos de entrega.
- O gerenciamento de grupos de entrega requer as permissões da função interna de Administrador de Grupo de Entrega. Para obter detalhes, consulte Administração delegada.

Geral

- Exibir detalhes do grupo
- Alterar propriedades preferenciais
- Alterar o tipo de entrega
- Alterar endereços do StoreFront™
- Alterar o nível funcional
- Gerenciar grupos de entrega do Acesso Remoto para PC
- Alterar a licença de um grupo de entrega
- Organizar grupos de entrega usando pastas
- Gerenciar proteção de aplicativos
- Alterar a capacidade de suspensão para um grupo de entrega

Exibir detalhes do grupo

1. Use a função de pesquisa para localizar um grupo de entrega específico. Consulte Pesquisar instâncias para obter instruções.
2. Nos resultados da pesquisa, selecione um grupo conforme necessário.
3. Consulte a tabela a seguir para obter descrições das colunas do grupo.
4. Clique em uma guia no painel de detalhes inferior para obter mais informações sobre este grupo.

COLUNA	DESCRIÇÃO
Grupo de Entrega	O nome do grupo e o tipo de sessão. Os tipos de sessão incluem SO de sessão única e SO de múltiplas sessões.
Entregando	O tipo de recursos entregues por este grupo. Os valores possíveis incluem Aplicativos, Desktops e Aplicativos e Desktops. "Atribuição de máquina estática" aparece se o grupo de entrega consistir em máquinas dedicadas.
Sessão em Uso	O número de máquinas configuradas e o número de máquinas que estão em estado Desconectado.
Contagem Alocada	O número de máquinas no catálogo atribuídas a um grupo de entrega.
Pasta	O local do grupo na árvore de **Grupos de Entrega**. Ele exibe o nome da pasta em que o grupo está (incluindo a barra invertida final), ou `-` se o grupo estiver no nível raiz.

Alterar propriedades preferenciais

As propriedades preferenciais controlam como os usuários acessam e iniciam recursos de um grupo de entrega. Para alterar as propriedades preferenciais de um grupo de entrega, siga estas etapas:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.

3. Na página **Preferências**, altere qualquer uma das configurações na tabela a seguir.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, selecione **OK** para aplicar as alterações e fechar a janela.

CONFIGURAÇÃO	DESCRIÇÃO
Descrição	O texto que os usuários finais veem.
Habilitar Grupo de Entrega	Se o grupo de entrega está habilitado.
Fuso horário	O fuso horário em que as máquinas deste grupo de entrega residem. Essa configuração mostra automaticamente o fuso horário definido em **Configurações > Data e Hora** para um grupo de entrega recém-criado. Você pode escolher um fuso horário diferente para o grupo de entrega, se necessário. O menu suspenso lista os fusos horários suportados pelo site. **Nota:** Alterar o fuso horário em um grupo de entrega pode reiniciar as máquinas nesse grupo de entrega. Para evitar isso, certifique-se de alterar as configurações de fuso horário fora do horário de produção.
Habilitar Secure ICA®	Protege as comunicações de e para as máquinas no grupo de entrega usando SecureICA, que criptografa o protocolo ICA. O nível padrão

CONFIGURAÇÃO	DESCRIÇÃO
	é de 128 bits. O nível pode ser alterado usando o SDK. A Citrix® recomenda usar mais métodos de criptografia, como a criptografia TLS, ao atravessar redes públicas. Além disso, o SecureICA não verifica a integridade dos dados.

Alterar o tipo de entrega de um grupo de entrega

O tipo de entrega indica o que o grupo pode entregar: aplicativos, desktops ou ambos.

Antes de alterar um tipo de **aplicativos** para o tipo de **Desktops**, exclua todos os aplicativos do grupo.

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. Na página **Tipo de Entrega**, selecione o tipo de entrega desejado.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, selecione **OK** para aplicar as alterações e fechar a janela.

Alterar endereços do StoreFront

1. No Studio, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. Na página **StoreFront**, indique se você especificará um endereço de servidor StoreFront mais tarde (**Manualmente**) ou selecione **Adicionar novo** para especificar os servidores StoreFront que você deseja usar (**Automaticamente**).
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, selecione **OK** para aplicar as alterações e fechar a janela.

Você também pode especificar endereços de servidor StoreFront na guia **Configurações** dentro do nó **Delivery Groups**.

Alterar o nível funcional

Altere o nível funcional do grupo de entrega depois de atualizar os VDAs em suas máquinas e os catálogos de máquinas que contêm as máquinas usadas no grupo de entrega.

Antes de começar:

- Se você usa o Citrix Provisioning™ (anteriormente Provisioning Services), atualize a versão do VDA no console do Citrix Provisioning.
- Inicie as máquinas que contêm o VDA atualizado para que elas possam se registrar no Citrix DaaS. Esse processo informa ao console o que deve ser alterado no grupo de entrega.
- Se você precisar continuar a usar versões anteriores do VDA, os recursos mais recentes do produto podem não estar disponíveis. Para obter mais informações, consulte a documentação de atualização.

Para alterar o nível funcional de um grupo de entrega:

1. No Studio, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Alterar Nível Funcional** na barra de ações. A ação **Alterar Nível Funcional** aparece somente se VDAs atualizados forem detectados.

A exibição indica quais máquinas, se houver, não podem ser alteradas para o nível funcional e por quê. Você pode então cancelar a ação de alteração, resolver os problemas da máquina e, em seguida, executar a ação de alteração novamente.

Após a conclusão da alteração, você pode reverter as máquinas para seus estados anteriores. Selecione o grupo de entrega e, em seguida, selecione **Desfazer Alteração de Nível Funcional** na barra de ações.

Gerenciar grupos de entrega do Remote PC Access

Se uma máquina em um catálogo de máquinas do Remote PC Access não estiver atribuída a um usuário, a máquina será temporariamente atribuída a um grupo de entrega associado a esse catálogo. Essa atribuição temporária permite que a máquina seja atribuída a um usuário posteriormente.

A associação do grupo de entrega ao catálogo de máquinas tem um valor de prioridade. A prioridade determina a qual grupo de entrega a máquina é atribuída quando se registra no sistema ou quando um usuário precisa de uma atribuição de máquina: quanto menor o valor, maior a prioridade. Se um catálogo de máquinas do Remote PC Access tiver várias atribuições de grupo

de entrega, o software selecionará a correspondência com a maior prioridade. Use o SDK do PowerShell para definir esse valor de prioridade.

Quando criados pela primeira vez, os catálogos de máquinas do Remote PC Access são associados a um grupo de entrega. Essa associação significa que as contas de máquina ou Unidades Organizacionais adicionadas ao catálogo posteriormente podem ser adicionadas ao grupo de entrega. Essa associação pode ser desativada ou ativada.

Para adicionar ou remover uma associação de catálogo de máquinas do Remote PC Access com um grupo de entrega:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo do Remote PC Access.
3. Na seção **Detalhes**, selecione a guia **Catálogos de Máquinas** e, em seguida, selecione um catálogo do Remote PC Access.
4. Para adicionar ou restaurar uma associação, selecione **Adicionar Desktops**. Para remover uma associação, selecione **Remover Associação**.

Alterar a licença para um grupo de entrega

Para alterar o direito de licença para um grupo de entrega, siga estas etapas:

1. Selecione **Grupos de Entrega** no painel de navegação.
2. Selecione um grupo e, em seguida, clique em **Editar** na barra de ações.
3. Na página **Atribuição de Licença**, selecione a licença que você deseja que o grupo use.
4. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Para obter mais informações sobre direitos de nível de grupo de entrega, consulte Licenças.

Organizar grupos de entrega usando pastas

Crie pastas para organizar os grupos de entrega para facilitar o acesso.

> **Dica:**
>
> Você pode definir sua exibição padrão preferida (exibição de pasta ou lista) para o nó Grupos de Entrega clicando no ícone **Pasta** no canto superior direito da barra de ações.

Funções necessárias

Por padrão, você precisa ter a seguinte função interna para criar e gerenciar pastas de grupo de entrega: Administrador de Nuvem, Administrador Completo ou Administrador de Grupo de Entrega. Se necessário, você pode personalizar as funções para criar e gerenciar pastas de grupo de entrega. Para obter mais informações, consulte Permissões necessárias.

Criar uma pasta de grupo de entrega

Antes de começar, planeje como organizar seus grupos de entrega. Considere o seguinte:

- Você pode aninhar pastas em até cinco níveis (*excluindo* a pasta de nó padrão).
- Uma pasta pode conter grupos de entrega e subpastas.
- Todos os nós no Studio (como **Catálogos de Máquinas**, **Grupos de Entrega**, **Aplicativos** e **Grupos de Aplicativos**) compartilham a mesma árvore de pastas no back-end. Para evitar conflitos de nomes ao renomear ou mover pastas, use nomes exclusivos para pastas de primeiro nível em diferentes nós.

  Se você criar uma pasta usando o cmdlet SDK `New-BrokerAdminFolder` e quiser que ela apareça sob o nó **Grupos de Entrega**, você deve adicionar os metadados `ContainsDeliveryGroups` usando o cmdlet `Set-BrokerAdminFolderMetadata`.

  Exemplo:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsDeliveryGroups -Value true
  ```

Para criar uma pasta de grupo de entrega, siga estas etapas:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione **Criar Pasta** na barra **Ação**.
3. Insira um nome para a nova pasta e, em seguida, clique em **Concluído**.

Dica:

Se você criar uma pasta em um local não intencional, poderá arrastá-la para o local correto.

Mover um grupo de entrega

Você pode mover um grupo de entrega entre pastas. As etapas detalhadas são as seguintes:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Visualize os grupos por pasta. Você também pode ativar **Ver todos** acima da hierarquia de pastas para visualizar todos os grupos de uma vez.
3. Clique com o botão direito do mouse em um grupo e, em seguida, selecione **Mover Grupo de Entrega**.
4. Selecione a pasta para a qual deseja mover o grupo e, em seguida, clique em **Concluído**.

> **Dica:**
>
> Você pode arrastar um grupo para uma pasta.

Gerenciar pastas de grupos de entrega

Você pode excluir, renomear e mover pastas de grupos de entrega.

Você pode excluir uma pasta somente se ela e suas subpastas não contiverem grupos de entrega.

Para gerenciar uma pasta, siga estas etapas:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Na hierarquia de pastas, selecione uma pasta e, em seguida, selecione uma ação na barra **Ação** conforme necessário:
   - Para renomear a pasta, selecione **Renomear Pasta**.
   - Para excluir a pasta, selecione **Excluir Pasta**.
   - Para mover a pasta, selecione **Mover Pasta**.
3. Siga as instruções na tela para concluir as etapas restantes.

Permissões necessárias

A tabela a seguir lista as permissões necessárias para executar ações em pastas de grupos de entrega.

AÇÃO	PERMISSÕES NECESSÁRIAS
Criar pastas de grupos de entrega	Criar Pasta de Grupo de Entrega
Excluir pastas de grupo de entrega	Remover Pasta de Grupo de Entrega
Mover pastas de grupo de entrega	Mover Pasta de Grupo de Entrega
Renomear pastas de grupo de entrega	Editar Pasta de Grupo de Entrega
Mover grupos de entrega para pastas	Editar Pasta de Grupo de Entrega e Editar Propriedades do Grupo de Entrega

Gerenciar proteção de aplicativos

As informações a seguir são complementares ao artigo Proteção de aplicativos na documentação do Citrix Virtual Apps and Desktops. Para usar a proteção de aplicativos em uma implantação do Citrix DaaS, siga as orientações gerais desse artigo, observando os seguintes detalhes.

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. Na página **Proteção de Aplicativos**, você pode ver as seguintes opções:

OPÇÕES	DESCRIÇÃO
Não aplicar	Selecione esta opção para não aplicar a configuração.
Aplicar a este grupo de entrega	Selecione as opções **Anti-keylogging** e/ou **Anti key capturing**. Passe o mouse sobre cada uma dessas configurações para ler os detalhes na dica de ferramenta.
Aplicar contextualmente	Para aplicar esta configuração, configure a política de acesso na página **Configurações da Política de Acesso**.
	1. Clique em **Política de Acesso** no painel esquerdo e clique em **Adicionar**.
	1. Na página **Adicionar Política**, faça o seguinte

OPÇÕES	DESCRIÇÃO
	- i. Insira um **Nome da política** e configure as configurações conforme necessário.
	- ii. Nos campos **Filtro** e **Valor**, insira os detalhes e clique em **Concluído**. A nova política é listada na página **Proteção de Aplicativos**. Habilite as configurações necessárias para esta política.
	- iii. Clique em **Salvar**.

4. Na página **Delivery Group**, selecione o **Delivery Group** e clique na guia **Details** na parte inferior. As novas configurações de **App Protection** aplicadas são exibidas.

- Você deve ter uma assinatura válida do Citrix Cloud™ e direitos válidos de proteção de aplicativos. Para adquirir o recurso de proteção de aplicativos, você pode entrar em contato com seu representante de vendas da Citrix.
- A proteção de aplicativos requer confiança XML. Para habilitar a confiança XML, vá para **Settings > Site settings > Enable XML trust**.
- Em relação à captura anti-tela:
  - No Windows e macOS, apenas a janela do conteúdo protegido fica em branco. A proteção de aplicativos está ativa quando uma janela protegida não está minimizada.
  - No Linux, a captura inteira fica em branco. A proteção de aplicativos está ativa, esteja uma janela protegida minimizada ou não.

Alterar a capacidade de suspensão para um grupo de entrega

Torne a capacidade de suspensão obrigatória ou opcional para um grupo de entrega:

- **Obrigatório**: O grupo de entrega só pode incluir VMs que são capazes de suspensão.
- **Opcional**: O grupo de entrega pode incluir VMs que são ou não capazes de suspensão.

Antes de começar

Você só pode alterar a capacidade de suspensão de um grupo de entrega para `Required` se todas as VMs presentes no grupo de entrega forem capazes de suspensão.

Para alterar a capacidade de suspensão de um grupo de entrega:

1. No Studio, vá para **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, clique em **Alterar Capacidade de Suspensão** na barra de ações.

Usuários

> **Nota:**
>
> A opção **Deixar o gerenciamento de usuários para o Citrix Cloud** foi removida. Para gerenciar atribuições de usuários para grupos de entrega existentes definidos como **Deixar o gerenciamento de usuários para o Citrix Cloud**, consulte Gerenciar atribuições de usuários para grupos de entrega gerenciados pela Biblioteca do Citrix Cloud.

Este tópico aborda as seguintes seções:

- Adicionar ou remover usuários
- Gerenciar atribuições de usuários para grupos de entrega gerenciados pela Biblioteca do Citrix Cloud
- Restringir o acesso do usuário a desktops e aplicativos em um grupo de entrega
- Restringir o acesso do usuário a recursos em um grupo de entrega
- Restringir o acesso do usuário a recursos em todos os grupos de entrega
- Configurar o escopo do usuário para uma política de acesso

Adicionar ou remover usuários em um grupo de entrega

Para obter informações detalhadas sobre usuários, consulte Usuários.

1. No Studio, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar Grupo de Entrega** na barra de ações.
3. Na página **Usuários**:
    - Para adicionar usuários, selecione **Adicionar** e, em seguida, especifique os usuários que deseja adicionar.
    - Para remover usuários, selecione um ou mais usuários e, em seguida, selecione **Remover**.

- Marque ou desmarque a caixa de seleção para permitir o acesso por usuários não autenticados.

4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, selecione **OK** para aplicar as alterações e fechar a janela.

Gerenciar atribuições de usuário para grupos de entrega gerenciados pela Biblioteca do Citrix Cloud

Para grupos de entrega gerenciados pela Biblioteca do Citrix Cloud, você pode gerenciar suas atribuições de usuário usando a Configuração Completa. As etapas detalhadas são as seguintes:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo de entrega gerenciado pela Biblioteca do Citrix Cloud e, em seguida, selecione **Editar** na barra de ações.
3. Para restringir o uso de um desktop a determinados usuários, siga estas etapas:
    a. Na página **Desktops** ou **Regras de Atribuição de Desktop**, selecione o desktop e clique em **Editar**. A página **Editar Desktop** é exibida com a opção **Restringir uso do desktop** selecionada.
    b. Clique em **Adicionar**, selecione os usuários conforme necessário e, em seguida, clique em **Concluído**.
    c. Clique em **OK**.
4. Para restringir o uso de aplicativos neste grupo a determinados usuários, clique em **Regra de Atribuição de Aplicativo** e siga as etapas semelhantes descritas na etapa 3 para adicionar usuários.

Restringir o acesso a desktops e aplicativos em um grupo de entrega

Você pode gerenciar o acesso do usuário aos recursos em um grupo de entrega executando as seguintes tarefas:

- Restringir o acesso a desktops a usuários específicos
- Restringir o acesso a aplicativos a usuários específicos

Restringir o acesso a desktops a usuários específicos

Os usuários que atendem *a ambas* as seguintes condições podem acessar desktops em um grupo de entrega:

- Ter acesso a recursos (aplicativos e desktops) neste grupo de entrega.

Por padrão, o acesso é determinado pela lista de acesso de usuário da implantação, que não é configurada via Studio. Você pode adicionar ou remover usuários do escopo de usuário padrão. Consulte Adicionar ou remover usuários em um grupo de entrega.

- Ter acesso a desktops neste grupo.

  Para obter mais informações, consulte Página Desktops (ou Regras de Atribuição de Desktop).

Para restringir o acesso a um desktop a usuários específicos, consulte Página Desktops (ou Regras de Atribuição de Desktop).

Restringir o acesso a aplicativos a usuários específicos

Os usuários que atendem *a todas* as seguintes condições podem acessar aplicativos em um grupo de entrega:

- Ter acesso a recursos (aplicativos e desktops) neste grupo de entrega.

  Por padrão, o acesso é determinado pela lista de acesso de usuário da implantação, que não é configurada via Studio. Você pode adicionar ou remover usuários do escopo de usuário padrão. Consulte Adicionar ou remover usuários em um grupo de entrega.

- Ter acesso a aplicativos neste grupo.

  Por padrão, a regra de política de direito de aplicativo inclui todos. Consulte os cmdlets `BrokerAppEntitlementPolicyRule` do PowerShell SDK para obter detalhes. Se necessário, você pode restringir o acesso do usuário a aplicativos em um grupo de entrega usando as etapas descritas abaixo.

- Ter acesso a grupos de aplicativos que incluem este aplicativo.

Para restringir o acesso a aplicativos para usuários específicos no nível do grupo de entrega, siga estas etapas:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo de entrega e, em seguida, selecione **Editar** na barra de ações.
3. Para restringir o acesso a aplicativos, siga estas etapas:
   a. No painel esquerdo, clique em **Regra de Atribuição de Aplicativo**.
   b. Para permitir que usuários específicos acessem aplicativos, selecione **Restringir uso de aplicativo** e, em seguida, clique em **Adicionar** na área **Lista de permissões** e especifique os usuários ou grupos de usuários a serem incluídos.

c. Para bloquear usuários específicos de acessar aplicativos, clique em **Adicionar** na área **Lista de bloqueios** e especifique os usuários ou grupos de usuários a serem excluídos.

Nota:

- Se você selecionar **Restringir uso de aplicativo** mas deixar as listas de permissões e de bloqueios vazias, nenhum usuário poderá usar aplicativos neste grupo.
- Se você selecionar **Restringir uso de aplicativo** e deixar a lista de permissões vazia, todos os usuários, exceto os usuários na **Lista de bloqueios**, poderão usar os aplicativos.

Restringir o acesso a recursos em um grupo de entrega

Quaisquer alterações feitas para restringir o acesso a recursos em um grupo de entrega substituem as configurações anteriores, independentemente do método usado. Você pode:

- **Restringir acesso para administradores usando escopos de administração delegada:** Você pode criar e atribuir um escopo que permite aos administradores acessar todos os aplicativos e outro escopo que fornece acesso apenas a determinados aplicativos. Para obter detalhes, consulte Administração delegada.
- **Restringir acesso para usuários por meio de expressões de política de acesso inteligente:** Você pode configurar regras de política de acesso para controlar o acesso do usuário a um grupo de entrega específico. Os exemplos incluem:
  - Restringir o acesso a um subconjunto de usuários e especificar os dispositivos de usuário permitidos.
  - Restringir o acesso a usuários conectados por meio de lojas na nuvem (em vez de lojas locais).
  - Restringir o acesso a usuários conectados por meio de um URL de loja específico.

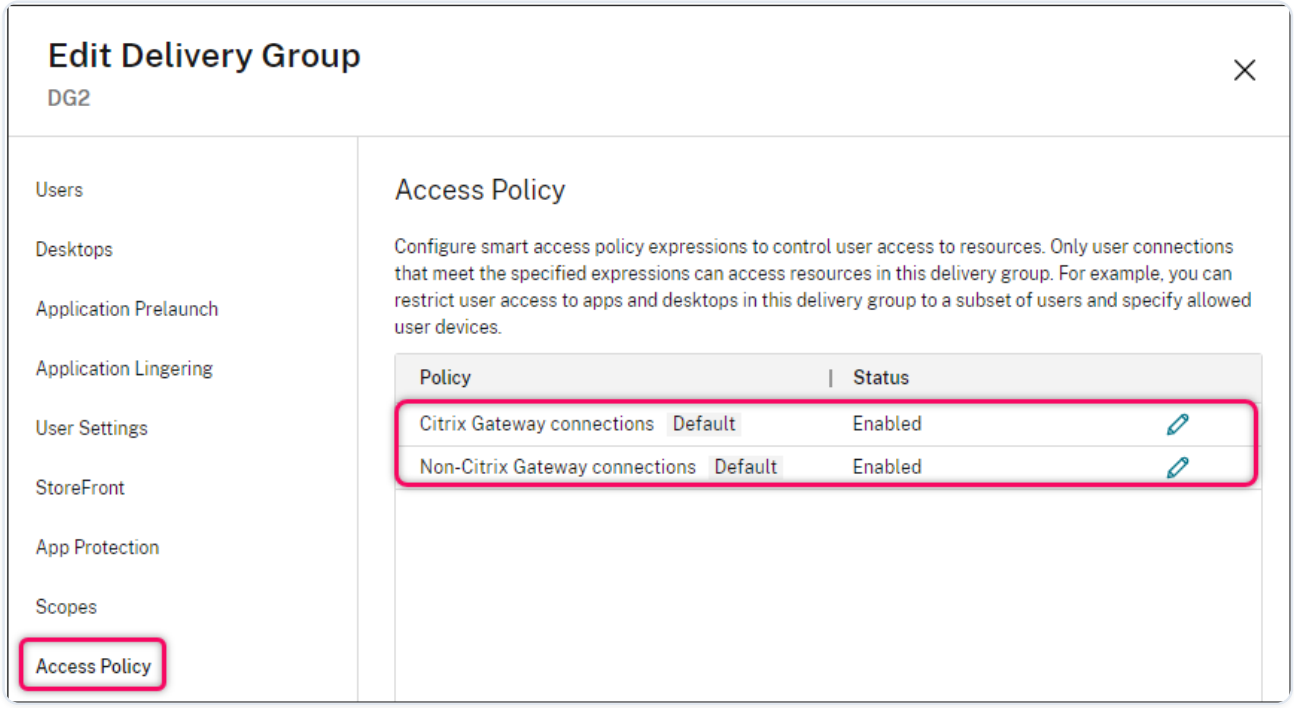
Esta seção o orienta sobre como restringir o acesso do usuário a grupos de entrega por meio de regras de política de acesso:

- Sobre as regras de política de acesso
- Adicionar regras de política de acesso
- Gerenciar regras de política de acesso usando o Studio
- Adicionar e refinar regras de política usando o PowerShell

Sobre as regras de política de acesso

Você pode configurar várias regras de política de acesso para um grupo de entrega. Aplicativos e desktops em um grupo de entrega aparecem no StoreFront ou Workspace de um usuário quando a conexão do usuário corresponde a qualquer regra de política de acesso que você definiu para o grupo de entrega, independentemente da ordem.

Cada regra pode ser ativada ou desativada individualmente. Uma regra desativada é ignorada quando a política de acesso é avaliada.



No Studio, a lista de Política de Acesso inclui as seguintes regras de política SmartAccess padrão. Você pode adicionar mais conforme necessário.

- **Conexões do Citrix Gateway.** Esta política permite que apenas conexões de usuário feitas através do Citrix Gateway acessem recursos dentro do grupo de entrega. Conexões de usuário feitas através do Workspace, quando os recursos de Postura do Dispositivo ou Localização de Rede estão habilitados, também são consideradas conexões através do Citrix Gateway.
- **Conexões que não são do Citrix Gateway.** Esta política permite que apenas conexões de usuário que não são feitas através do Citrix Gateway acessem recursos dentro do grupo de entrega.

> **Nota:**

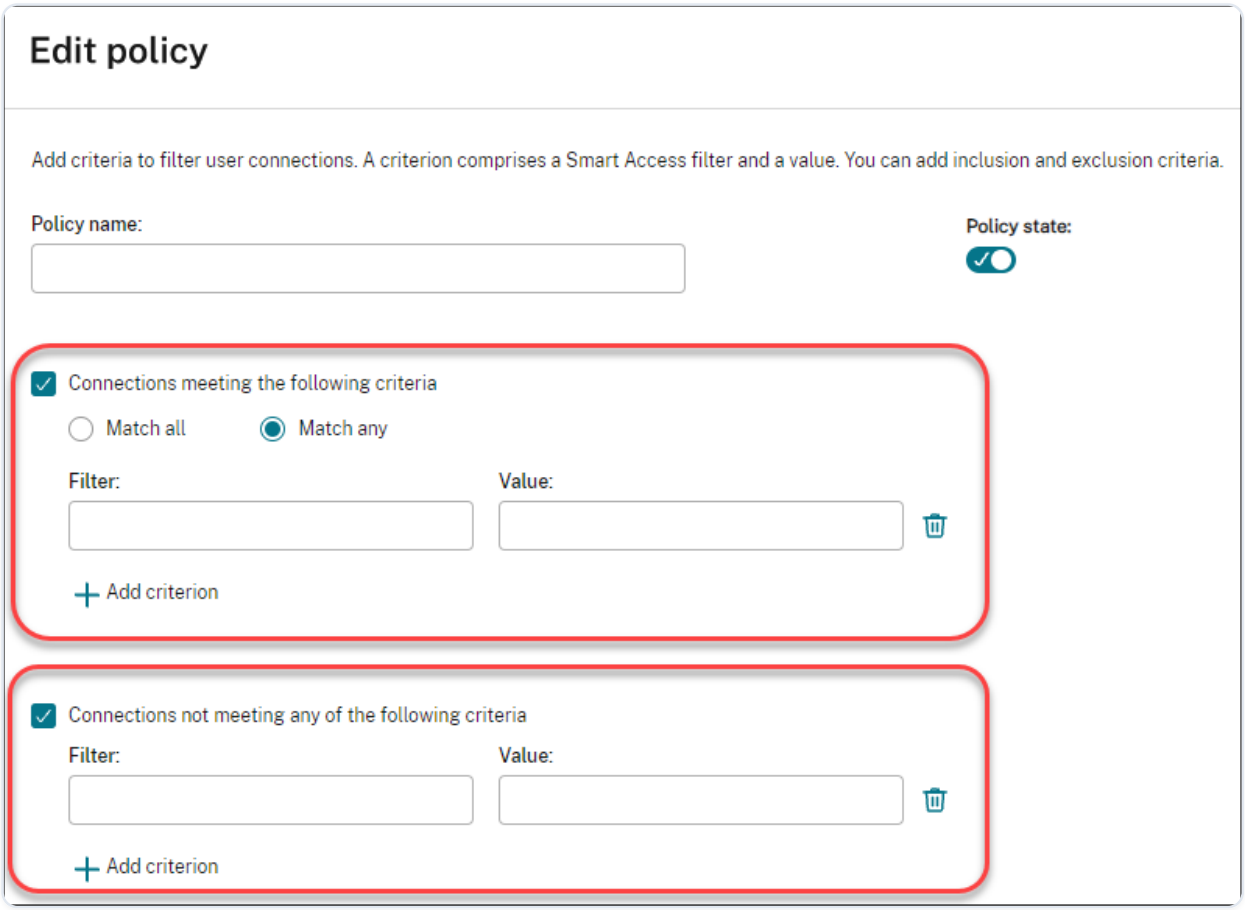
- Para evitar que as regras padrão substituam uma recém-configurada, você deve desabilitar as regras padrão ou refiná-las para excluir os filtros usados na nova política.
- As políticas padrão não podem ser excluídas, mas podem ser desabilitadas. Para desabilitar uma política, clique no ícone **Editar** e, em seguida, altere o **Estado da política** para **Desabilitado**.
- A lista de políticas também mostra as regras adicionadas usando comandos do PowerShell. Essas políticas podem ser excluídas, mas não podem ser editadas no Studio.

Adicionar regras de política de acesso usando o Studio

Uma regra de política de acesso compreende um conjunto de filtros. Para obter mais informações sobre filtros, consulte este artigo. Ao adicionar uma regra de política de acesso, você adiciona vários filtros de condição à regra conforme necessário.

Para adicionar uma política para um grupo de entrega usando o Studio, siga estas etapas:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e clique em **Editar** na barra de ações.
3. Na página **Política de Acesso**, clique em **Adicionar**. A página **Adicionar Política** é exibida.



4. No campo **Nome da política**, digite um nome descritivo para a política. O nome deve ser exclusivo em sua implantação.
5. Para definir os critérios para conexões de usuário permitidas, siga estas etapas:
   a. Selecione **Conexões que atendem aos seguintes critérios**.
   b. Clique em **Adicionar critério**.
   c. No campo **Filtro**, digite o nome do filtro que você deseja usar. No campo **Valor**, digite um valor desejado para o filtro. Por exemplo, para permitir que apenas usuários conectados via Workspace (em vez de StoreFront) acessem recursos neste grupo de entrega, digite `Citrix-Via-Workspace` para **Filtro** e `True` para **Valor**.
   d. Para adicionar mais critérios, repita as etapas b-c.
   e. Selecione o relacionamento entre os critérios:
      - **Corresponder a qualquer**. Permite o acesso somente quando a conexão de usuário de entrada atende a qualquer um dos critérios de filtro configurados.
      - **Corresponder a todos**. Permite o acesso somente quando a conexão de usuário de entrada atende a todos os critérios de filtro configurados.
6. Para definir os critérios para conexões de usuário proibidas, siga estas etapas:

a. Selecione **Conexões que não atendem a nenhum dos seguintes critérios**.

b. Clique em **Adicionar critério**.

c. No campo **Filtro**, digite o nome do filtro que você deseja usar. No campo **Valor**, digite um valor desejado para o filtro. Por exemplo, para proibir que usuários conectados por meio da URL da loja `example.cloud.com` acessem recursos neste grupo de entrega. Digite `Citrix.Workspace.UsingDomain` para **Filtro** e `example.cloud.com` para **Valor**.

d. Para adicionar mais critérios, repita as etapas b-c.

> **Nota:**
>
> As conexões de usuário que atendem a qualquer um dos critérios configurados são proibidas de acessar recursos neste grupo de entrega.

7. Clique em **Concluído**.

   A nova política aparece na lista de políticas.

8. Revise e refine as regras de política padrão para evitar sobreposições não intencionais com conexões cobertas por esta nova política. Para refinar as políticas existentes, use as seguintes maneiras:

   - Desative as regras de política padrão.
   - Configure as regras de política padrão para excluir os filtros SmartAccess que você adicionou aos critérios de inclusão da nova política. Para obter mais informações, consulte Gerenciar regras de política usando o Studio e Adicionar e gerenciar regras de política de acesso usando o PowerShell.

> **Importante:**
>
> Conforme explicado em Sobre as regras de política de acesso, quando a conexão de um usuário corresponde a uma ou mais regras de política em um grupo de entrega, o usuário obtém acesso aos seus recursos. Portanto, após criar uma regra, você deve revisar e refinar cuidadosamente as regras existentes para evitar sobreposições não intencionais com conexões cobertas pela nova regra.

Gerenciar regras de política de acesso usando o Studio

Você pode usar os critérios de inclusão e exclusão para refinar as políticas padrão. Por exemplo, para restringir o acesso a um subconjunto dessas conexões, siga estas etapas:

1. Edite uma política padrão.
2. Selecione **Conexões que atendem a qualquer um dos seguintes critérios**.
3. Adicione, edite ou remova as expressões de política SmartAccess para os cenários de acesso de usuário permitidos.

Para obter mais informações, consulte a documentação do Citrix Gateway.

Adicionar e gerenciar regras de política de acesso usando o PowerShell

Você pode usar os seguintes cmdlets do PowerShell para adicionar e gerenciar regras de política de acesso para grupos de entrega:

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- Rename-BrokerAccessPolicyRule
- Remove-BrokerAccessPolicyRule

Para obter mais informações, consulte os artigos relacionados na Citrix Developer Documentation.

Restringir o acesso do usuário a recursos em todos os grupos de entrega

Você pode configurar regras de filtragem de recursos para controlar o acesso do usuário a aplicativos e desktops em todos os grupos de entrega. Essas regras permitem especificar o tipo de recurso, aplicar restrições baseadas em tags e impor condições de acesso com base em fatores como localização de rede e contexto de conexão da loja.

Permissão necessária

Para executar esta tarefa, você deve ter uma função de administrador com a permissão **Gerenciar filtro de recursos**.

Adicionar uma regra de filtragem de recursos

Para adicionar uma regra de filtragem de recursos, siga as etapas abaixo:

1. Vá para **Grupos de Entrega > Configurações**.
2. Selecione **Gerenciar** no bloco **Filtro de recursos**.

3. Na caixa de diálogo **Gerenciar regras de filtro de recursos**, clique em **Adicionar**.
4. Insira um **Nome** e uma **Descrição** para a regra.
5. Selecione o tipo de recurso ao qual a regra se aplica:
   - **Aplicativos**
   - **Desktops**
   - **Ambos**
6. Selecione a tag que identifica os recursos aos quais a regra se aplica.

> **Nota:**
>
> Se você selecionar **Ambos** como o tipo de recurso, a seleção de uma tag é obrigatória.

7. Configure o **filtro Smart Access** para definir as condições sob as quais os recursos são filtrados.
8. Clique em **Adicionar** para salvar a regra.

Configurar escopo de usuário para uma política de acesso

Por padrão, todas as políticas de acesso em um grupo de entrega se aplicam ao mesmo conjunto de usuários. Você pode configurar uma política de acesso para se aplicar a usuários específicos usando o Studio, PowerShell ou a API Rest.

Para aplicar uma política de acesso a usuários especificados usando o Studio, siga estas etapas:

1. No Studio, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit Delivery Group** na barra de ações.
3. Na página **Users**, selecione **Use contextual access.**
4. Selecione a política de acesso que você deseja configurar e clique em **Escopo de acesso do usuário**. A página **Escopo de acesso do usuário** é exibida.
5. Para definir a quais usuários autenticados esta política se aplica:
   - Para aplicar esta política a *quaisquer* usuários autenticados, selecione **Permitir que quaisquer usuários autenticados usem recursos**.

- Para aplicar esta política a usuários específicos, mantenha **Restringir o uso de recursos** selecionado. Em seguida, use a lista de permissões e a lista de bloqueios para adicionar ou remover usuários para esta política.

6. Para aplicar esta política de acesso a usuários que não fornecem credenciais, selecione **Conceder acesso a usuários não autenticados (anônimos); nenhuma credencial é necessária**.

Máquinas

- Gerenciar atribuições de usuário para máquinas
- Habilitar Cache de Host Local para VDAs agrupados de sessão única
- Atualizar uma máquina
- Adicionar, alterar ou remover uma restrição de tag para um desktop
- Remover uma máquina
- Impedir que usuários se conectem a uma máquina (modo de manutenção)
- Desligar e reiniciar máquinas
- Criar e gerenciar agendamentos de reinício para máquinas
- Habilitar um agendamento de reinício único
- Gerenciar Autoscale™

Além dos recursos descritos neste artigo, consulte Autoscale para obter informações sobre o gerenciamento proativo de energia das máquinas.

Gerenciar atribuições de usuário para máquinas

> **Nota:**
>
> Esta tarefa está disponível apenas para máquinas estáticas de sessão única provisionadas por MCS.

Gerencie as atribuições de usuário para máquinas em um grupo de entrega. Quando as regras de atribuição de desktop são configuradas para o grupo de entrega, as máquinas são atribuídas aleatoriamente aos usuários no lançamento inicial do desktop e permanecem atribuídas aos usuários, a menos que suas atribuições de usuário sejam modificadas. Se você deseja atribuir manualmente uma máquina não atribuída a usuários específicos ou

> alterar a atribuição de usuário existente para uma máquina, siga as etapas descritas nesta tarefa para fazer as alterações. Usando essas etapas, você também pode modificar os nomes exibidos no Citrix Workspace App para máquinas atribuídas a usuários.

As etapas detalhadas são as seguintes:

1. No Studio, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. No painel esquerdo, selecione **Machine Allocation**. Os seguintes detalhes para cada máquina no grupo aparecem:
   - **Nome da máquina:** Mostra o nome de uma máquina.
   - **Nome de exibição:** Mostra o nome de exibição da máquina no Citrix Workspace App.
   - **Usuários:** Mostra os usuários atribuídos a esta máquina. Se as regras de atribuição de desktop forem configuradas, as máquinas serão atribuídas aleatoriamente aos usuários no lançamento inicial do desktop e permanecerão atribuídas a eles, a menos que suas atribuições de usuário sejam modificadas.
4. Localize uma máquina e, em seguida, atribua usuários a ela ou altere sua atribuição de usuário:
   - Clique em **Browser** para navegar até os usuários.
   - Na coluna **Usuários**, insira uma lista de nomes de usuário separados por ponto e vírgula.
   - Clique em **Importar do arquivo CSV** para importar os detalhes da configuração usando um arquivo CSV.
   - Clique em **Alterar** para atualizar o ícone da área de trabalho da máquina a partir de um arquivo `.ico` ou `.exe`. O ícone especificado substitui o conjunto de ícones padrão apenas no nível da máquina.
5. (Opcional) Se a máquina for atribuída a usuários, modifique seu nome de exibição conforme necessário.

   > **Nota:**
   >
   > O campo Nome de exibição é habilitado somente quando a máquina é atribuída a usuários:

- Se a máquina for atribuída a um usuário com base em uma regra de atribuição de área de trabalho, este campo mostrará o nome de exibição configurado nessa regra.
- Se a máquina for atribuída manualmente a usuários e o campo for deixado em branco, o nome publicado do grupo de entrega (se especificado) será usado como o nome de exibição da máquina. O nome do grupo de entrega será usado se o nome publicado não for especificado. Você pode especificar nomes publicados para grupos de entrega somente via PowerShell.

6. Selecione **Aplicar** para aplicar as alterações e manter a janela aberta. Ou, selecione **OK** para aplicar as alterações e fechar a janela.

Habilitar Cache de Host Local para VDAs agrupados de sessão única

Por padrão, máquinas agrupadas, de sessão única e gerenciadas por energia podem ser usadas para apenas uma sessão quando no modo Cache de Host Local. Você pode substituir o comportamento padrão por grupo de entrega. As etapas detalhadas são as seguintes:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo conforme necessário e, em seguida, selecione **Editar** na barra de ações.
3. Na página **Cache de Host Local**, selecione **Usar máquinas para sessões subsequentes**.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, selecione **OK** para aplicar as alterações e fechar a janela.

Alternativamente, você pode substituir o comportamento padrão usando comandos PowerShell. Para obter mais informações, consulte Habilitar usando PowerShell.

Importante:

Habilitar o acesso a máquinas agrupadas de sessão única com gerenciamento de energia pode fazer com que dados e alterações de sessões de usuário anteriores estejam presentes em sessões subsequentes.

Atualizar uma máquina em um grupo de entrega

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Exibir Máquinas** na barra de ações.

3. Selecione uma máquina e, em seguida, selecione **Atualizar Máquinas** na barra de ações.

Para escolher uma imagem diferente, selecione **Imagem** e, em seguida, selecione um instantâneo.

Para aplicar as alterações e notificar os usuários da máquina, selecione **Notificação de lançamento para usuários finais**. Em seguida, especifique:

- Quando atualizar a imagem: agora ou na próxima reinicialização
- O tempo de distribuição da reinicialização (o tempo total para começar a atualizar todas as máquinas no grupo)
- Se os usuários são notificados da reinicialização
- A mensagem que os usuários receberão

Adicionar, alterar ou remover uma restrição de tag para um desktop

Adicionar, alterar e remover restrições de tag pode ter efeitos inesperados sobre quais desktops são considerados para lançamento. Revise as considerações e precauções em Tags.

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de Ações.
3. Na página **Desktops**, selecione o desktop e selecione **Editar**.
4. Para adicionar uma restrição de tag, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag.
5. Para alterar ou remover uma restrição de tag, faça o seguinte:
    - Selecione uma tag diferente.
    - Remova a restrição de tag desmarcando **Restringir inicializações a máquinas com esta tag**.
6. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, selecione **OK** para aplicar as alterações e fechar a janela.

Remover uma máquina de um grupo de entrega

Remover uma máquina a exclui de um grupo de entrega. Isso não a exclui do catálogo de máquinas que o grupo de entrega usa. Portanto, essa máquina está disponível para atribuição a outro grupo de entrega.

As máquinas devem ser desligadas antes de serem removidas. Para impedir temporariamente que os usuários se conectem a uma máquina enquanto você a remove, coloque a máquina em modo de manutenção antes de desligá-la.

As máquinas podem conter dados pessoais, portanto, tenha cuidado antes de alocar a máquina para outro usuário. Considere refazer a imagem da máquina.

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Exibir Máquinas** na barra de ações.
3. Certifique-se de que a máquina esteja desligada.
4. Selecione a máquina e, em seguida, selecione **Remover do Grupo de Entrega** na barra de ações.

Você também pode remover uma máquina de um grupo de entrega através da conexão que a máquina usa.

Impedir que usuários se conectem a uma máquina (modo de manutenção) em um grupo de entrega

Quando você precisa interromper temporariamente novas conexões com máquinas, pode ativar o modo de manutenção para uma ou todas as máquinas em um grupo de entrega. Você pode fazer isso antes de aplicar patches ou usar ferramentas de gerenciamento.

- Quando uma máquina de SO multi-sessão está no modo de manutenção, os usuários podem se conectar a sessões existentes, mas não podem iniciar novas sessões.
- Quando uma máquina de SO de sessão única (ou um PC usando Acesso Remoto a PC) está no modo de manutenção, os usuários não podem se conectar ou reconectar. As conexões atuais permanecem conectadas até que se desconectem ou façam logoff.

Para ativar ou desativar o modo de manutenção:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo.
3. Para ativar o modo de manutenção para todas as máquinas no grupo de entrega, selecione **Ativar Modo de Manutenção** na barra de ações.

   Para ativar o modo de manutenção para uma máquina, selecione **Exibir Máquinas** na barra de ações. Selecione uma máquina e, em seguida, selecione **Ativar Modo de Manutenção** na barra de ações.

4. Para desativar o modo de manutenção para uma ou todas as máquinas em um grupo de entrega, siga as instruções anteriores, mas selecione **Desativar Modo de Manutenção** na barra de ações.

As configurações da Conexão de Área de Trabalho Remota (RDC) do Windows também afetam se uma máquina de SO multi-sessão está no modo de manutenção. O modo de manutenção é ativado quando ocorre qualquer um dos seguintes:

- O modo de manutenção está ativado, conforme descrito anteriormente.
- A RDC está configurada para **Não permitir conexões a este computador**.
- O RDC não está definido como **Não permitir conexões a este computador** e a configuração do Modo de Logon do Usuário de Configuração do Host Remoto é **Permitir reconexões, mas impedir novos logons** ou **Permitir reconexões, mas impedir novos logons até que o servidor seja reiniciado**.

Você também pode ativar ou desativar o modo de manutenção para:

- Uma conexão, o que afeta as máquinas que usam essa conexão.
- Um catálogo de máquinas, o que afeta as máquinas nesse catálogo.

Desligar e reiniciar máquinas em um grupo de entrega

Este procedimento não é suportado para máquinas de Acesso Remoto a PC.

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Exibir Máquinas** na barra de ações.
3. Selecione a máquina e, em seguida, selecione uma das seguintes ações na barra de ações:

> **Nota:**
>
> - As seguintes ações se aplicam apenas a máquinas que são gerenciadas por energia.
> - Algumas opções podem não estar disponíveis, dependendo do estado da máquina.

- **Forçar desligamento:** Desliga a máquina à força e atualiza a lista de máquinas.
- **Reiniciar:** Solicita ao sistema operacional que desligue e, em seguida, inicie a máquina novamente. Se o sistema operacional não puder cumprir, a máquina permanecerá em seu estado atual.

- **Forçar reinício:** Desliga o sistema operacional à força e, em seguida, reinicia a máquina.
- **Suspender:** Pausa a máquina sem desligá-la e atualiza a lista de máquinas.
- **Desligar:** Solicita ao sistema operacional que seja desligado.

Para ações não forçadas, se a máquina não desligar em 10 minutos, ela será desligada. Se o Windows tentar instalar atualizações durante o desligamento, há o risco de a máquina ser desligada antes que as atualizações sejam concluídas.

Criar e gerenciar agendamentos de reinicialização para máquinas em um grupo de entrega

> **Nota:**
>
> - Quando um agendamento de reinicialização é aplicado a um grupo de entrega com o Autoscale ativado, suas máquinas são apenas desligadas e deixadas para o Autoscale ligá-las.
> - Quando os agendamentos de reinicialização são aplicados a máquinas aleatórias de sessão única, essas máquinas são desligadas em vez de reiniciadas, para economizar custos. Recomendamos que você use o Autoscale para ligar as máquinas.
> - Alterar o fuso horário em um grupo de entrega pode reiniciar as máquinas nesse grupo de entrega. Para evitar isso, certifique-se de alterar as configurações de fuso horário fora do horário de produção.

> Um agendamento de reinicialização especifica quando as máquinas em um grupo de entrega são reiniciadas periodicamente. Você pode criar um ou mais agendamentos para um grupo de entrega. Um agendamento pode afetar:

- Todas as máquinas do grupo.
- Uma ou mais (mas não todas) máquinas do grupo. As máquinas são identificadas por uma tag que você aplica à máquina. Isso é chamado de restrição de tag, porque a tag restringe uma ação apenas a itens (neste caso, máquinas) que possuem a tag.

Por exemplo, digamos que todas as suas máquinas estejam em um grupo de entrega. Você deseja que cada máquina seja reiniciada uma vez por semana e que as máquinas usadas pela equipe de contabilidade sejam reiniciadas diariamente. Para conseguir isso, configure um

agendamento para todas as máquinas e outro agendamento apenas para as máquinas da contabilidade.

Um agendamento inclui o dia e a hora em que a reinicialização começa e a duração. A duração é "iniciar todas as máquinas afetadas ao mesmo tempo" ou um intervalo que provavelmente levará para reiniciar todas as máquinas afetadas.

Você pode ativar ou desativar um agendamento. Desativar um agendamento pode ser útil durante testes, em intervalos especiais ou ao preparar agendamentos antes de precisar deles.

Você não pode usar agendamentos para ligar ou desligar automaticamente a partir do console de gerenciamento, apenas para reiniciar.

Sobreposição de agendamentos

Vários agendamentos podem se sobrepor. No exemplo acima, ambos os agendamentos afetam as máquinas de contabilidade. Essas máquinas podem ser reiniciadas duas vezes no domingo. O código de agendamento foi projetado para evitar reiniciar a mesma máquina com mais frequência do que o pretendido, mas isso não pode ser garantido.

- Se os agendamentos coincidirem precisamente nos horários de início e duração, é mais provável que as máquinas sejam reiniciadas apenas uma vez.
- Quanto mais os agendamentos diferirem nos horários de início e duração, mais provável será que ocorram várias reinicializações.
- O número de máquinas afetadas por um agendamento também afeta a chance de uma sobreposição. No exemplo, o agendamento semanal que afeta todas as máquinas pode iniciar reinicializações mais rapidamente do que o agendamento diário para máquinas de contabilidade, dependendo da duração especificada para cada um.

Para uma análise aprofundada dos agendamentos de reinicialização, consulte Detalhes internos do agendamento de reinicialização.

Exibir agendamentos de reinicialização

1. No Studio, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. Selecione a página **Agendamento de Reinicialização**.

A página **Agendamento de Reinicialização** contém as seguintes informações para cada agendamento configurado:

- Nome do agendamento.

- Restrição de tag usada, se houver.
- Com que frequência as reinicializações da máquina ocorrem.
- Se os usuários da máquina recebem uma notificação.
- Se o agendamento está ativado. Desativar um agendamento pode ser útil durante testes, em intervalos especiais ou ao preparar agendamentos antes que sejam necessários.

Adicionar (aplicar) tags

Ao configurar um agendamento de reinício que usa uma restrição de tag, certifique-se de que a tag foi adicionada (aplicada) às máquinas que o agendamento afeta. No exemplo acima, cada uma das máquinas usadas pela equipe de contabilidade tem uma tag aplicada. Para obter detalhes, consulte Tags.

Embora você possa aplicar mais de uma tag a uma máquina, um agendamento de reinício pode especificar apenas uma tag.

1. No Studio, selecione **Delivery Groups** no painel esquerdo.
2. Selecione o grupo que contém as máquinas a serem controladas pelo agendamento.
3. Selecione **View Machines** e, em seguida, selecione as máquinas às quais você deseja adicionar uma tag.
4. Selecione **Manage Tags** na barra de ações.
5. Se a tag existir, marque a caixa de seleção ao lado do nome da tag. Se a tag não existir, selecione **Create** e, em seguida, especifique o nome da tag. Depois que a tag for criada, marque a caixa de seleção ao lado do nome da tag recém-criada.
6. Selecione **Save** na caixa de diálogo **Manage Tags**.

Criar um agendamento de reinício

> **Nota:**
>
> Os agendamentos de reinício podem ser aplicados a todas as máquinas multissessão gerenciadas por energia e não gerenciadas por energia.

1. No Studio, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit** na barra de ações.
3. Na página **Restart Schedule**, selecione **Add**.

4. Na página **Add Restart Schedule**:

   - Para habilitar o agendamento, selecione **Yes**. Para desabilitar o agendamento, selecione **No**.
   - Digite um nome e uma descrição para o agendamento.
   - Para **Restrict to tag**, aplique uma restrição de tag.
   - Para **Include machines in maintenance mode**, escolha se deseja incluir máquinas que estão no modo de manutenção neste agendamento. Para usar o PowerShell, consulte Reinicializações agendadas para máquinas em modo de manutenção.
   - Para **Restart frequency**, selecione a frequência com que a reinicialização ocorre: diariamente, semanalmente, mensalmente ou uma vez. Se você selecionar **Weekly** ou **Monthly**, poderá especificar um ou mais dias específicos.
   - Para **Repeats every**, especifique a frequência com que você deseja que o agendamento seja executado.
   - Para **Start date**, especifique uma data de início para a primeira ocorrência do agendamento.
   - Para **Begin restart at**, especifique, no formato de 24 horas, a hora do dia para iniciar a reinicialização.
   - Para **Restart duration**:

     - Para reiniciar máquinas à força com sessões que não respondem, selecione **Forced restart** e, em seguida, selecione uma das seguintes opções:

       - **Reiniciar todas as máquinas de uma vez**
       - **Reiniciar todas as máquinas dentro de um período de tempo** e especificar o tempo por **Hour** ou **Minute**.

     - Para aguardar que todas as sessões sejam encerradas antes de reiniciar, selecione **Graceful restart**.

       Ao iniciar um agendamento de reinício configurado para usar reinício suave:

       - Todas as máquinas ociosas pertencentes ao grupo de entrega são reiniciadas imediatamente
       - Cada máquina pertencente à entrega com uma ou mais sessões ativas é reiniciada quando todas as sessões são desconectadas.

> **Nota:**
>
> Os agendamentos de reinício suave só podem reiniciar máquinas gerenciadas por energia.

- Em **Enviar notificação aos usuários**, determine se deseja exibir uma mensagem de notificação nas máquinas aplicáveis antes do início de um reinício. Por padrão, nenhuma mensagem é exibida.
- Se você optar por exibir uma mensagem 15 minutos antes do início do reinício, poderá optar por repetir a mensagem a cada cinco minutos após a mensagem inicial. Por padrão, a mensagem não se repete.
- Insira o título e o texto da notificação. Não há texto padrão.

  Se você quiser que a mensagem inclua uma contagem regressiva para o reinício, inclua a variável **%m%**. A menos que você tenha escolhido reiniciar todas as máquinas ao mesmo tempo, a mensagem aparecerá em cada máquina no momento apropriado antes do reinício.

5. Clique em **Concluído** para aplicar as alterações e fechar a janela **Adicionar Agendamento de Reinício**.
6. Clique em **Aplicar** para aplicar as alterações feitas e manter a janela **Editar Grupo de Entrega** aberta. Ou, clique em **Salvar** para aplicar as alterações e fechar a janela.

Executar um agendamento de reinício imediatamente

Um agendamento de reinício especifica quando as máquinas em um grupo de entrega reiniciam regularmente. Você também pode executar um agendamento de reinício imediatamente para reiniciar as máquinas nesse agendamento.

Para executar um agendamento de reinício imediatamente, siga estas etapas:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione o grupo de entrega aplicável e, em seguida, selecione **Editar** na barra de ações
3. Na página **Reiniciar Agendamento**, selecione um agendamento que você deseja executar e, em seguida, selecione **Executar agendamento agora**.

> **Nota:**

- Você não pode executar um agendamento imediatamente se ele estiver configurado com a configuração **Reiniciar todas as máquinas após o esgotamento das sessões**.
- Você pode aplicar **Executar agendamento agora** apenas a um agendamento por vez.
- Depois de editar um agendamento, **Executar agendamento agora** fica indisponível. Selecione **Aplicar** para torná-lo disponível.

Editar, remover, habilitar ou desabilitar um agendamento de reinicialização

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. Na página **Reiniciar Agendamento**, selecione a caixa de seleção de um agendamento.
    - Para editar um agendamento, selecione **Editar**. Atualize a configuração do agendamento, usando as orientações em Criar um agendamento de reinicialização.
    - Para habilitar ou desabilitar um agendamento, selecione **Editar**. Marque ou desmarque a caixa de seleção **Habilitar agendamento de reinicialização**.
    - Para remover um agendamento, selecione **Remover**. Confirme a remoção. A remoção de um agendamento não afeta nenhuma tag aplicada às máquinas nas máquinas afetadas.

Reinicializações agendadas atrasadas devido a interrupção do banco de dados

Nota:

Este recurso está disponível apenas no PowerShell.

Se ocorrer uma interrupção do banco de dados do site antes do início de uma reinicialização agendada para máquinas (VDAs) em um grupo de entrega, as reinicializações começarão quando a interrupção terminar. Essa ação pode ter resultados indesejados.

Por exemplo, digamos que você agendou as reinicializações de um grupo de entrega para ocorrerem fora do horário de produção (começando às 3h). Uma interrupção do banco de dados do site ocorre uma hora antes do início de uma reinicialização agendada (2h). A interrupção dura seis horas (até as 8h). O agendamento de reinicialização começa quando a conexão entre o Delivery Controller™ e o banco de dados do site é restaurada. As reinicializações do VDA agora

começam cinco horas após o agendamento original. Essa ação pode resultar em reinicializações de VDAs durante o horário de produção.

Para ajudar a evitar essa situação, você pode usar o parâmetro `MaxOvertimeStartMins` para os cmdlets `New-BrokerRebootScheduleV2` e `Set-BrokerRebootScheduleV2`. O valor especifica o número máximo de minutos além do horário de início agendado em que um agendamento de reinicialização pode começar.

- Se a conexão do banco de dados for restaurada dentro desse tempo (horário agendado + `MaxOvertimeStartMins`), as reinicializações do VDA começarão.
- Se a conexão do banco de dados não for restaurada dentro desse tempo, as reinicializações do VDA não começarão.
- Se este parâmetro for omitido ou tiver um valor zero, a reinicialização agendada começará quando a conexão com o banco de dados for restaurada, independentemente da duração da interrupção.

Para obter mais informações, consulte a ajuda do cmdlet. Este recurso está disponível apenas no PowerShell.

Reinicializações agendadas para máquinas em modo de manutenção

Para indicar se um agendamento de reinicialização afeta máquinas que estão em modo de manutenção, use a opção `IgnoreMaintenanceMode` com os cmdlets `BrokerRebootScheduleV2`.

Por exemplo, o cmdlet a seguir cria um agendamento que reinicia tanto as máquinas que estão quanto as que não estão em modo de manutenção.

```
New-BrokerRebootSchedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup>
-IgnoreMaintenanceMode $true
```

O cmdlet a seguir modifica um agendamento de reinicialização existente.

```
Set-BrokerRebootSchedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

Para obter mais informações, consulte a ajuda do cmdlet.

Habilitar um agendamento de reinicialização único

Se você quiser habilitar um agendamento de reinicialização único usando o PowerShell, use os seguintes comandos `BrokerCatalogRebootSchedule` do PowerShell para criar, modificar e excluir um agendamento de reinicialização:

- `Get-BrokerCatalogRebootSchedule`
- `New-BrokerCatalogRebootSchedule`
- `Set-BrokerCatalogRebootSchedule`
- `Remove-BrokerCatalogRebootSchedule`
- `Rename-BrokerCatalogRebootSchedule`

Limitações:

- Um agendamento de reinicialização de catálogo associado a um catálogo sem um fuso horário configurado é criado, mas não é iniciado.
- Quando um agendamento de reinicialização de catálogo é criado, o agendamento de reinicialização é executado apenas nas VMs do catálogo pertencentes a um grupo de entrega.

Exemplo:

- Para criar um agendamento de reinicialização das VMs no catálogo chamado **BankTellers** para começar em Feb 3, 2022, entre 2h e 4h.

```
New-BrokerCatalogRebootSchedule -Name BankTellers

-CatalogName BankTellers

-StartDate "2022-02-03"

-StartTime "02:00"

-Enabled $true

-RebootDuration 120
```

- Para criar um agendamento de reinicialização das VMs no catálogo com UID 17 para começar em Feb 3, 2022, entre 1h e 5h. Dez minutos antes da reinicialização, cada VM é configurada para exibir uma caixa de mensagem com o título: **AVISO: Reinicialização pendente**, e a mensagem: **Salve seu trabalho**, em cada sessão de usuário.

```
New-BrokerCatalogRebootSchedule

-Name 'Update reboot'

-CatalogUid 17
```

```
-StartDate "2022-02-03"

-StartTime "01:00" -Enabled $true -RebootDuration 240

-WarningTitle "WARNING: Reboot pending"

-WarningMessage "Save your work" -WarningDuration 10
```

- Para renomear o agendamento de reinicialização do catálogo chamado **Nome Antigo** para **Novo Nome**.

```
Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName "New Name"
```

- Para exibir todos os agendamentos de reinicialização de catálogo com UID 1 e, em seguida, renomear o agendamento de reinicialização de catálogo com o UID 1 para **Novo Nome**.

```
Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- Para definir o agendamento de reinicialização do catálogo chamado **Accounting** para exibir uma mensagem com o título **AVISO: Reinicialização pendente, e a mensagem, Salve seu trabalho**, dez minutos antes da reinicialização de cada VM. A mensagem aparece em cada sessão de usuário nessa VM.

```
Set-BrokerCatalogRebootSchedule -Name Accounting

-WarningMessage "Save your work"

-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
```

- Para exibir todos os agendamentos de reinicialização desabilitados e, em seguida, habilitar todos os agendamentos de reinicialização desabilitados.

```
Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- Para definir o agendamento de reinicialização do catálogo com UID 17 para exibir a mensagem: **Reiniciando em %m% minutos** quinze, dez e cinco minutos antes da reinicialização de cada VM.

```
Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in %m%
minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- Para configurar o fuso horário para o catálogo chamado **MyCatalog**.

```
Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
```

Gerenciar Autoscale

Por padrão, o Autoscale está desabilitado para grupos de entrega. Para gerenciar o Autoscale para um grupo de entrega (se aplicável), siga estas etapas:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Gerenciar Autoscale** na barra de ações. A janela **Gerenciar Autoscale** é exibida.
3. Configure as configurações conforme necessário. Para obter informações sobre as configurações do Autoscale, consulte Autoscale.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta. Ou, selecione **Salvar** para aplicar as alterações e fechar a janela.

Sessões

- Fazer logoff ou desconectar uma sessão, ou enviar uma mensagem aos usuários
- Configurar o pré-lançamento e a permanência da sessão
- Configurar o roaming de sessão
- Controlar a reconexão da sessão quando desconectado da máquina em modo de manutenção

Fazer logoff ou desconectar uma sessão, ou enviar uma mensagem para usuários do grupo de entrega

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Exibir Máquinas** na barra de ações.

3. Para fazer logoff de um usuário de uma sessão, selecione a sessão ou área de trabalho e, em seguida, selecione **Logoff** na barra de ações. A sessão é encerrada e a máquina fica disponível para outros usuários, a menos que esteja alocada a um usuário específico.
4. Para desconectar uma sessão, selecione a sessão ou área de trabalho e, em seguida, selecione **Desconectar** na barra de ações. Os aplicativos continuam em execução e a máquina permanece alocada a esse usuário. O usuário pode se reconectar à mesma máquina.
5. Para enviar uma mensagem aos usuários, selecione a sessão, máquina ou usuário e, em seguida, selecione **Enviar mensagem** na barra de ações. Digite a mensagem.

Configurar o pré-lançamento e a permanência da sessão em um grupo de entrega

Esses recursos são suportados apenas em máquinas de SO multi-sessão.

Os recursos de pré-lançamento de sessão e permanência de sessão ajudam os usuários especificados a acessar aplicativos rapidamente, por meio de:

- Iniciando sessões antes que sejam solicitadas (pré-lançamento de sessão)
- Mantendo as sessões de aplicativo ativas depois que um usuário fecha todos os aplicativos (permanência de sessão)

Por padrão, o pré-lançamento de sessão e a permanência de sessão não são usados. Uma sessão é iniciada (lançada) quando um usuário inicia um aplicativo e permanece ativa até que o último aplicativo aberto na sessão seja fechado.

Considerações:

- O grupo de entrega deve suportar aplicativos, e as máquinas devem estar executando um VDA para SO multi-sessão, versão mínima 7.6.
- Esses recursos são suportados apenas ao usar o aplicativo Citrix Workspace para Windows e também exigem mais configuração do aplicativo Citrix Workspace. Para obter instruções, procure por pré-lançamento de sessão na documentação do produto para sua versão do aplicativo Citrix Workspace para Windows.
- O Citrix Workspace app para HTML5 não é compatível.
- Ao usar o pré-lançamento de sessão, se a máquina de um usuário for colocada em modo de suspensão ou hibernação, o pré-lançamento não funciona (independentemente das configurações de pré-lançamento de sessão). Os usuários podem bloquear suas máquinas/sessões. No entanto, se um usuário sair do Citrix Workspace app, a sessão é encerrada e o pré-lançamento não se aplica mais.

- Ao usar o pré-lançamento de sessão, as máquinas cliente físicas não podem usar as funções de gerenciamento de energia de suspensão ou hibernação. Os usuários da máquina cliente podem bloquear suas sessões, mas não devem fazer logoff.
- Se estiver usando uma licença de usuário/dispositivo, a licença dura 90 dias. As sessões pré-lançadas e persistentes não utilizadas são desconectadas após 15 minutos por padrão. Você pode configurar o valor de tempo limite no PowerShell (cmdlet `New/Set-BrokerSessionPreLaunch`).
- O planejamento e o monitoramento cuidadosos dos padrões de atividade dos seus usuários são essenciais para adaptar esses recursos para que se complementem. A configuração ideal equilibra os benefícios da disponibilidade antecipada de aplicativos para os usuários com o custo de manter as licenças em uso e os recursos alocados.
- Você também pode configurar o pré-lançamento de sessão para um horário agendado no Citrix Workspace app.

Por quanto tempo as sessões pré-lançadas e persistentes não utilizadas permanecem ativas

Existem várias maneiras de especificar por quanto tempo uma sessão não utilizada permanece ativa se o usuário não iniciar um aplicativo: um tempo limite configurado e limites de carga do servidor. Você pode configurar todos eles. O evento que ocorre primeiro faz com que a sessão não utilizada seja encerrada.

- **Tempo limite:** Um tempo limite configurado especifica o número de minutos, horas ou dias que uma sessão pré-lançada ou persistente não utilizada permanece ativa. Se você configurar um tempo limite muito curto, as sessões pré-lançadas terminam antes de fornecerem ao usuário o benefício de um acesso mais rápido ao aplicativo. Se você configurar um tempo limite muito longo, as conexões de usuário de entrada podem ser negadas porque o servidor não tem recursos suficientes.

  Você pode habilitar esse tempo limite apenas no SDK (cmdlet `New/Set-BrokerSessionPreLaunch`), não no console de gerenciamento. Se você desabilitar o tempo limite, ele não aparecerá na exibição do console para esse grupo de entrega ou nas páginas **Editar Grupo de Entrega**.
- **Limites:** O encerramento automático de sessões pré-lançadas e persistentes com base na carga do servidor garante que as sessões permaneçam abertas o maior tempo possível, assumindo que os recursos do servidor estejam disponíveis. As sessões pré-lançadas e persistentes não utilizadas não causam conexões negadas porque são encerradas automaticamente quando os recursos são necessários para novas sessões de usuário.

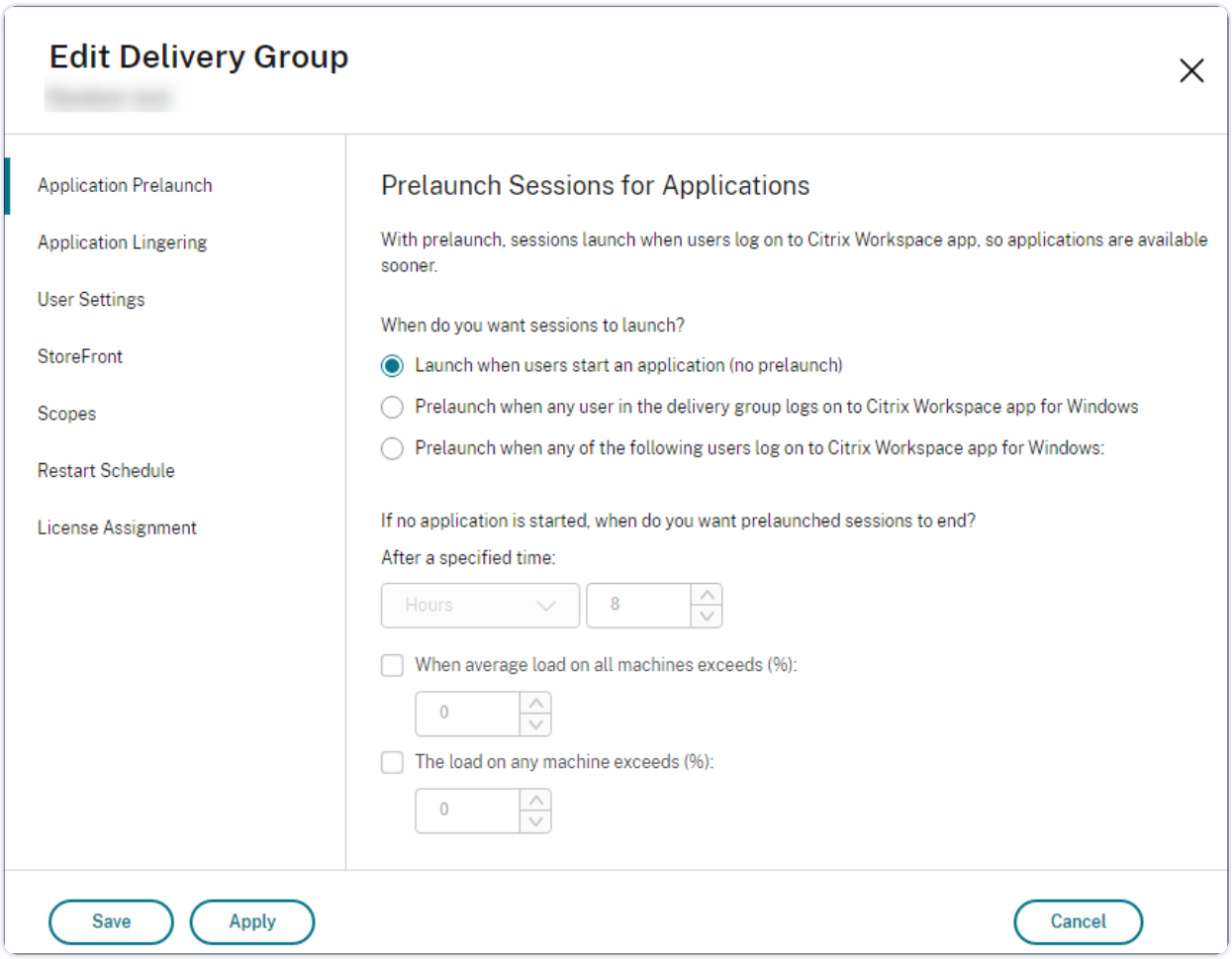
Você pode configurar dois limites: a porcentagem média de carga de todos os servidores no grupo de entrega e a porcentagem máxima de carga de um único servidor no grupo. Quando um limite é excedido, as sessões que estiveram no estado de pré-lançamento ou persistência por mais tempo são encerradas. As sessões são encerradas uma a uma em intervalos de um minuto até que a carga caia abaixo do limite. Enquanto o limite é excedido, nenhuma nova sessão de pré-lançamento é iniciada.

Servidores com VDAs que não se registraram em um Controller e servidores em modo de manutenção são considerados totalmente carregados. Uma interrupção não planejada faz com que as sessões de pré-lançamento e persistentes sejam encerradas automaticamente para liberar capacidade.

Para habilitar o pré-lançamento de sessão

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.
3. Na página **Pré-lançamento de Aplicativos**, ative o pré-lançamento de sessão escolhendo quando as sessões são iniciadas:

    - Quando um usuário inicia um aplicativo. Esta é a configuração padrão. O pré-lançamento de sessão está desativado.
    - Quando qualquer usuário no grupo de entrega faz logon no Citrix Workspace app para Windows.
    - Quando qualquer pessoa em uma lista de usuários e grupos de usuários faz logon no Citrix Workspace app para Windows. Certifique-se de especificar também usuários ou grupos de usuários se você escolher esta opção.



4. Uma sessão pré-lançada é substituída por uma sessão regular quando o usuário inicia um aplicativo. Se o usuário não iniciar um aplicativo (a sessão pré-lançada não for usada), as seguintes configurações afetam por quanto tempo essa sessão permanece ativa.

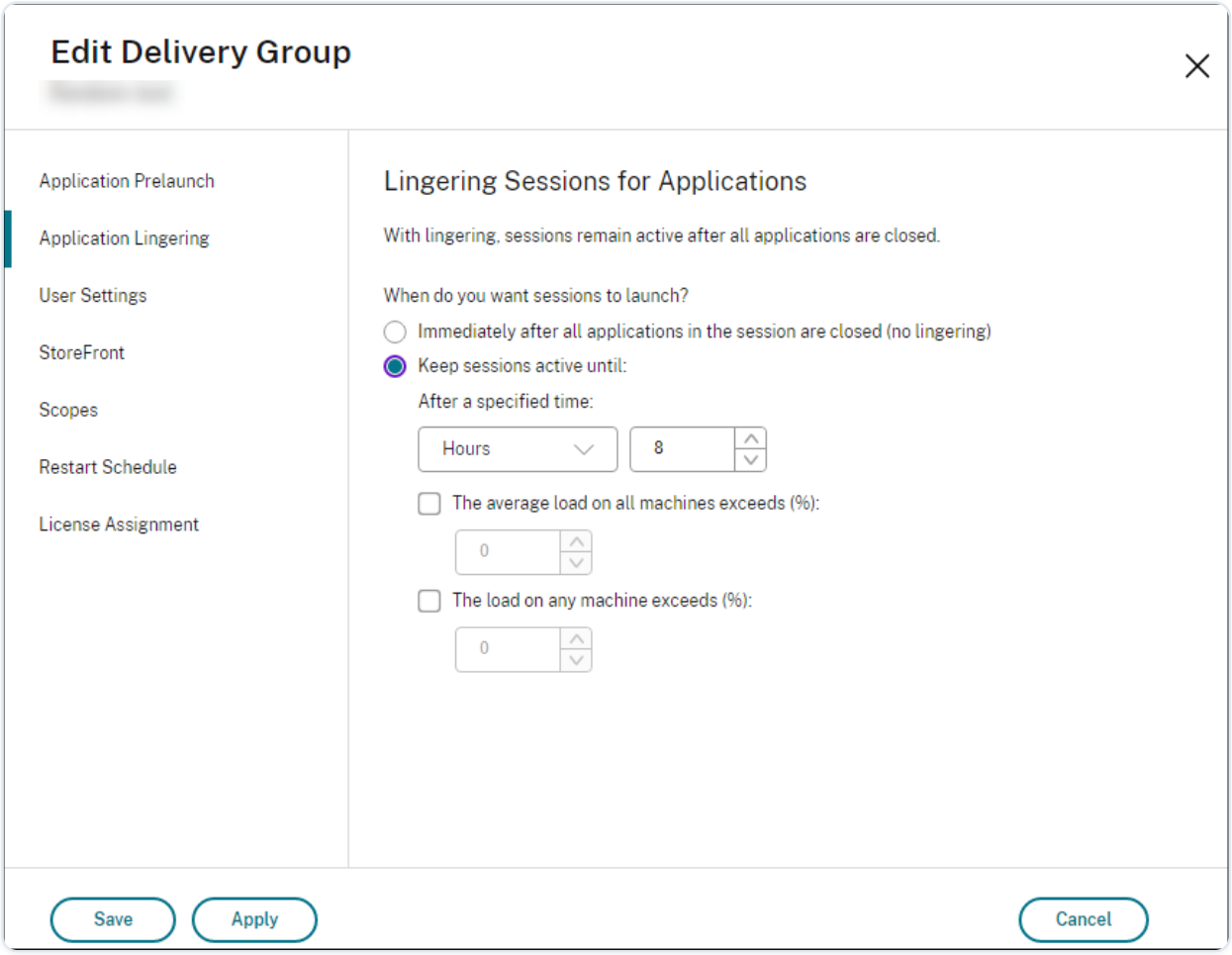
   - Quando um intervalo de tempo especificado decorre. Você pode alterar o intervalo de tempo (1–99 dias, 1–2376 horas ou 1–142.560 minutos).
   - Quando a carga média em todas as máquinas no grupo de entrega excede uma porcentagem especificada (1–99%).
   - Quando a carga em qualquer máquina no grupo de entrega excede uma porcentagem especificada (1–99%).

   Recapitulação: Uma sessão pré-lançada permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado decorre ou um limite de carga especificado é excedido.

Para habilitar a permanência da sessão

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar** na barra de ações.

3. Na página **Permanência do Aplicativo**, ative a permanência da sessão selecionando **Manter sessões ativas até**.



4. Várias configurações afetam por quanto tempo uma sessão persistente permanece ativa se o usuário não iniciar outro aplicativo.

   - Quando um intervalo de tempo especificado expira. Você pode alterar o intervalo de tempo: 1–99 dias, 1–2376 horas ou 1–142.560 minutos.
   - Quando a carga média em todas as máquinas no grupo de entrega excede uma porcentagem especificada: 1–99%.
   - Quando a carga em qualquer máquina no grupo de entrega excede uma porcentagem especificada: 1–99%.

   Recapitulação: Uma sessão persistente permanece ativa até que um dos seguintes eventos ocorra: um usuário inicia um aplicativo, o tempo especificado expira ou um limite de carga especificado é excedido.

Configurar o roaming de sessão

Por padrão, o roaming de sessão é habilitado para grupos de entrega. As sessões fazem roaming entre dispositivos cliente com o usuário. Quando o usuário inicia uma sessão e depois se move para outro dispositivo, a mesma sessão é usada e os aplicativos ficam simultaneamente disponíveis em ambos os dispositivos. Você pode visualizar os aplicativos em vários dispositivos. Os aplicativos seguem, independentemente do dispositivo ou se as sessões atuais existem. Frequentemente, impressoras e outros recursos atribuídos ao aplicativo também seguem. Alternativamente, você também pode usar o PowerShell. Para obter mais informações, consulte Roaming de sessão.

Configurar o roaming de sessão para aplicativos

Para configurar o roaming de sessão para aplicativos, siga estas etapas:

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Editar Grupo de Entrega** na barra de ações.
3. Na página **Usuários**, habilite o roaming de sessão selecionando a caixa de seleção **Sessões fazem roaming com os usuários à medida que eles se movem entre dispositivos**.
    - Quando habilitado, se um usuário iniciar uma sessão de aplicativo e depois se mover para outro dispositivo, a mesma sessão será usada e estará disponível em ambos os dispositivos. Quando desabilitado, a sessão não fará mais roaming entre os dispositivos.
4. Selecione **OK** para aplicar as alterações e fechar a janela.

Configurar roaming de sessão para desktops

Para configurar o roaming de sessão para um desktop, siga estas etapas:

1. No Studio, selecione **Delivery Groups** no painel esquerdo.
2. Selecione um grupo e, em seguida, selecione **Edit Delivery Group** na barra de ações.
3. Na página **Desktops**, selecione o desktop e selecione **Edit**.
4. Habilite o roaming de sessão selecionando a caixa de seleção **Session roaming**.
    - Quando ativado, se o usuário iniciar o desktop e depois mudar para outro dispositivo, a mesma sessão será usada e os aplicativos estarão disponíveis em ambos os dispositivos. Quando desativado, a sessão não faz mais roaming entre os dispositivos.
5. Selecione **OK** para aplicar as alterações e fechar a janela.

Controlar a reconexão de sessão quando desconectado da máquina em modo de manutenção

> **Nota:**
>
> Este recurso está disponível apenas no PowerShell.

> Você pode controlar se as sessões que são desconectadas em máquinas no modo de manutenção têm permissão para se reconectar a máquinas no grupo de entrega.

Antes do final de maio de 2021, a reconexão não era permitida para sessões de desktop agrupadas de sessão única que haviam sido desconectadas de máquinas em modo de manutenção. Agora, você pode configurar um grupo de entrega para permitir ou proibir reconexões (independentemente do tipo de sessão) após a desconexão de uma máquina em modo de manutenção.

Ao criar ou editar um grupo de entrega (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), use o parâmetro `-AllowReconnectInMaintenanceMode <boolean>` para permitir ou proibir reconexões para máquinas que foram desconectadas de uma máquina em modo de manutenção.

- Quando definido como true, as sessões podem se reconectar às máquinas do grupo.
- Quando definido como falso, as sessões não podem se reconectar às máquinas no grupo.

Valores padrão:

- Sessão única: Desabilitado
- Multi-sessão: Habilitado

Aplicativos

Visualize aplicativos em um grupo de entrega e adicione mais, se necessário.

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione um grupo. Se este grupo contiver aplicativos, **Visualizar Aplicativos** aparecerá na barra de ações.
3. Selecione **Visualizar Aplicativos**. Você será direcionado para o nó **Aplicativos**, onde todos os aplicativos disponíveis neste grupo aparecerão.

4. Para adicionar mais aplicativos a este grupo, vá para o nó **Grupos de Entrega**, selecione o grupo e selecione **Adicionar Aplicativos** na barra de ações.

Solução de problemas

- VDAs que não estão registrados em um Delivery Controller não são considerados ao iniciar sessões intermediadas. Isso resulta na subutilização de recursos que de outra forma estariam disponíveis. Existem várias razões pelas quais um VDA pode não estar registrado, muitas das quais um administrador pode solucionar. A exibição de detalhes fornece informações de solução de problemas no assistente de criação de catálogo e depois que você adiciona um catálogo a um grupo de entrega.

  Depois de criar um grupo de entrega, o painel de detalhes de um grupo de entrega indica o número de máquinas que deveriam estar registradas, mas não estão. Por exemplo, uma ou mais máquinas estão ligadas e não estão no modo de manutenção, mas não estão atualmente registradas em um Controller. Ao visualizar uma máquina "não registrada, mas deveria estar", revise a guia **Solução de problemas** no painel de detalhes para possíveis causas e ações corretivas recomendadas.

  Para mensagens sobre o nível funcional, consulte Versões de VDA e níveis funcionais.

  Para obter informações sobre a solução de problemas de registro de VDA, consulte CTX136668.

- Na exibição de um grupo de entrega, a **versão do VDA instalada** no painel de detalhes pode ser diferente da versão real instalada nas máquinas. A exibição de Programas e Recursos do Windows da máquina mostra a versão real do VDA.
- Para máquinas com status de **Estado de Energia Desconhecido**, consulte CTX131267 para obter orientação.

Criar grupos de aplicativos

Introdução

Os grupos de aplicativos permitem gerenciar coleções de aplicativos. Você pode criar grupos de aplicativos para aplicativos compartilhados entre diferentes grupos de entrega ou usados por um subconjunto de usuários dentro de grupos de entrega. Os grupos de aplicativos são opcionais. Eles oferecem uma alternativa para adicionar os mesmos aplicativos a vários grupos de entrega. Os grupos de entrega podem ser associados a mais de um grupo de aplicativos, e um grupo de aplicativos pode ser associado a mais de um grupo de entrega.

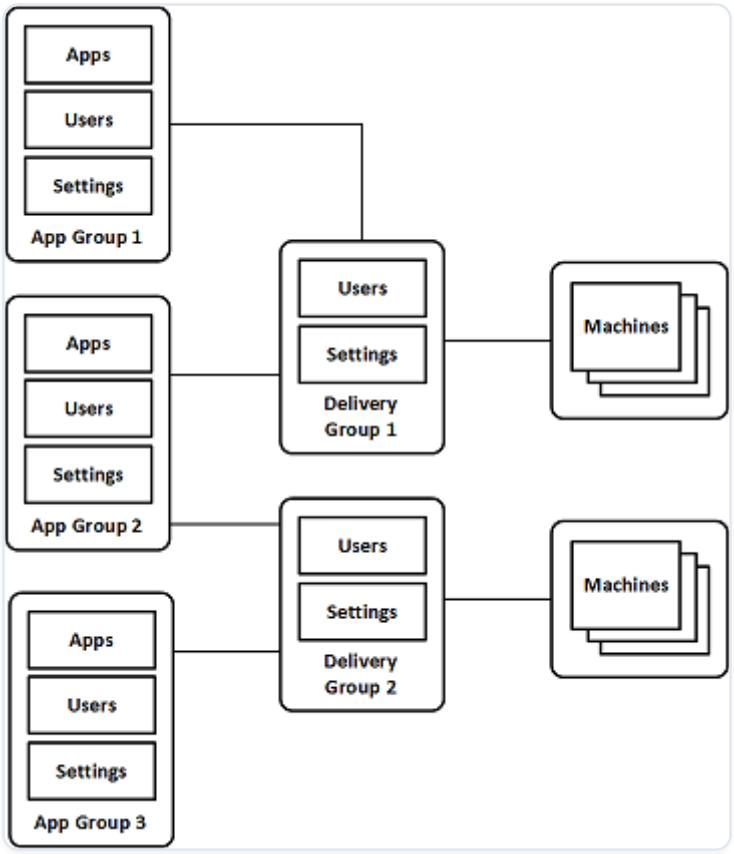
O uso de grupos de aplicativos pode oferecer vantagens de gerenciamento de aplicativos e controle de recursos em relação ao uso de mais grupos de entrega:

- O agrupamento lógico de aplicativos e suas configurações permite gerenciar esses aplicativos como uma única unidade. Por exemplo, você não precisa adicionar (publicar) o mesmo aplicativo a grupos de entrega individuais um por um.
- O compartilhamento de sessão entre grupos de aplicativos pode conservar o consumo de recursos. Em outros casos, desabilitar o compartilhamento de sessão entre grupos de aplicativos pode ser benéfico.
- Você pode usar o recurso de restrição de tags para publicar aplicativos de um grupo de aplicativos, considerando apenas um subconjunto das máquinas em grupos de entrega selecionados. Com restrições de tags, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando os custos associados à implantação e gerenciamento de máquinas adicionais. Uma restrição de tag pode ser considerada como a subdivisão (ou particionamento) das máquinas em um grupo de entrega. Usar um grupo de aplicativos ou desktops com uma restrição de tag pode ser útil ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.

Configurações de exemplo

Exemplo 1

O gráfico a seguir mostra uma implantação que inclui grupos de aplicativos:



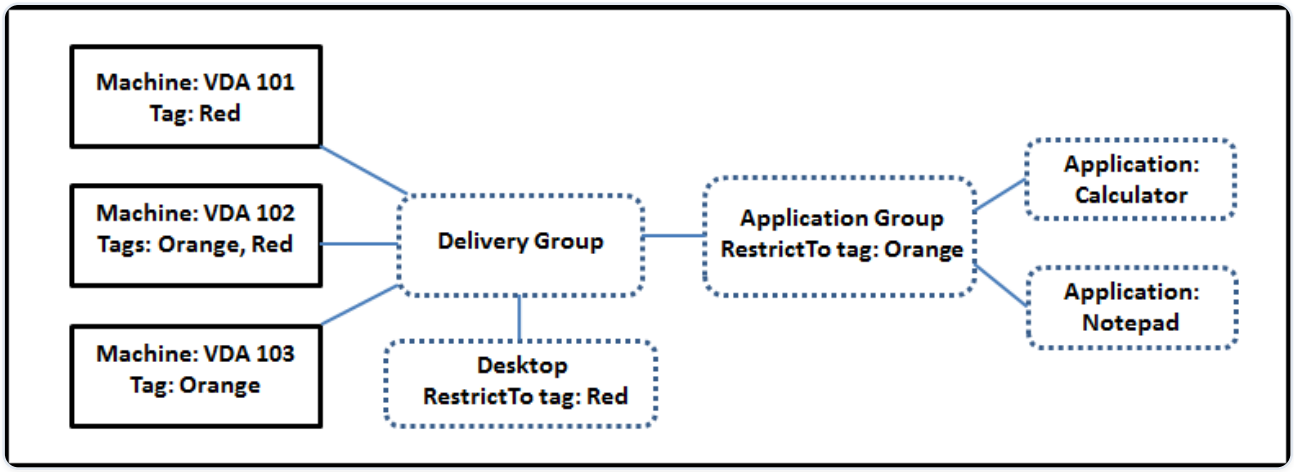
Nesta configuração, os aplicativos são adicionados aos grupos de aplicativos, não aos grupos de entrega. Os grupos de entrega especificam quais máquinas serão usadas. (Embora não mostrado, as máquinas estão em catálogos de máquinas.)

O grupo de aplicativos 1 está associado ao grupo de entrega 1. Os aplicativos no grupo de aplicativos 1 podem ser acessados pelos usuários especificados no grupo de aplicativos 1, desde que também estejam na lista de usuários do grupo de entrega 1. Isso segue a orientação de que a lista de usuários para um grupo de aplicativos deve ser um subconjunto (uma restrição) das listas de usuários para os grupos de entrega associados. As configurações no grupo de aplicativos 1 (como compartilhamento de sessão de aplicativo entre grupos de aplicativos, grupos de entrega associados) se aplicam a aplicativos e usuários nesse grupo. As configurações no grupo de entrega 1 (como suporte a usuários anônimos) se aplicam a usuários nos grupos de aplicativos 1 e 2, porque esses grupos de aplicativos foram associados a esse grupo de entrega.

O grupo de aplicativos 2 está associado a dois grupos de entrega: 1 e 2. Cada um desses grupos de entrega pode receber uma prioridade no grupo de aplicativos 2, o que indica a ordem em que os grupos de entrega serão verificados quando um aplicativo for iniciado. Grupos de entrega com prioridade igual são balanceados por carga. Os aplicativos no grupo de aplicativos 2 podem ser acessados pelos usuários especificados no grupo de aplicativos 2, desde que também estejam nas listas de usuários do grupo de entrega 1 e do grupo de entrega 2.

Exemplo 2

Este layout simples usa restrições de tag para limitar quais máquinas serão consideradas para determinados lançamentos de desktop e aplicativos. O site tem um grupo de entrega compartilhado, um desktop publicado e um grupo de aplicativos configurado com dois aplicativos.



Tags foram adicionadas a cada uma das três máquinas (VDA 101-103).

O grupo de aplicativos foi criado com a restrição de tag "Orange", então cada um de seus aplicativos (Calculadora e Bloco de Notas) pode ser iniciado apenas em máquinas nesse grupo de entrega que possuem a tag "Orange": VDA 102 e 103.

Para exemplos mais abrangentes e orientações sobre o uso de restrições de tag em grupos de aplicativos (e para desktops), consulte Tags.

Orientação e considerações

A Citrix® recomenda adicionar aplicativos a grupos de aplicativos ou grupos de entrega, mas não a ambos. Caso contrário, a complexidade adicional de ter aplicativos em dois tipos de grupo pode dificultar o gerenciamento.

Por padrão, um grupo de aplicativos é habilitado. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativo entre grupos de aplicativos é habilitado. Consulte Compartilhamento de sessão entre grupos de aplicativos.

A Citrix recomenda atualizar seus grupos de entrega para a versão atual. Isso requer:

1. Atualizar VDAs nas máquinas usadas no grupo de entrega.
2. Alterar para um nível de função superior para os catálogos de máquinas que contêm essas máquinas

3. Alterar para um nível de função superior para o grupo de entrega.

Para obter detalhes, consulte Gerenciar grupos de entrega.

Para usar grupos de aplicativos, seus componentes principais devem ser no mínimo da versão 7.9.

A criação de grupos de aplicativos requer a permissão de administração delegada da função interna de Administrador de Grupo de Entrega. Consulte Administração delegada para obter detalhes.

Este artigo se refere à "associação" de um aplicativo a mais de um grupo de aplicativos para diferenciar essa ação da adição de uma nova instância desse aplicativo a partir de uma fonte disponível. Da mesma forma, os grupos de entrega são associados a grupos de aplicativos (e vice-versa), em vez de serem adições ou componentes uns dos outros.

Compartilhamento de sessão com grupos de aplicativos

Quando o compartilhamento de sessão de aplicativo está habilitado, todos os aplicativos são iniciados na mesma sessão de aplicativo. Isso economiza os custos associados ao lançamento de sessões de aplicativo adicionais e permite o uso de recursos de aplicativo que envolvem a área de transferência, como operações de copiar e colar. No entanto, em algumas situações, você pode querer desativar o compartilhamento de sessão.

Ao usar grupos de aplicativos, você pode configurar o compartilhamento de sessão de aplicativo das três maneiras a seguir, que estendem o comportamento padrão de compartilhamento de sessão disponível ao usar apenas grupos de entrega:

- Compartilhamento de sessão habilitado entre grupos de aplicativos.
- Compartilhamento de sessão habilitado apenas entre aplicativos no mesmo grupo de aplicativos.
- Compartilhamento de sessão desabilitado.

Compartilhamento de sessão entre grupos de aplicativos

Você pode habilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos ou pode desabilitá-lo para limitar o compartilhamento de sessão de aplicativo apenas a aplicativos no mesmo grupo de aplicativos.

- **Um exemplo em que habilitar o compartilhamento de sessão entre grupos de aplicativos é útil:**

O Grupo de Aplicativos 1 contém aplicativos do Microsoft Office, como Word e Excel. O Grupo de Aplicativos 2 contém outros aplicativos, como Bloco de Notas e Calculadora, e ambos os grupos de aplicativos estão anexados ao mesmo grupo de entrega. Um usuário que tem acesso a ambos os grupos de aplicativos inicia uma sessão de aplicativo lançando o Word e, em seguida, lança o Bloco de Notas. Se a sessão existente do usuário executando o Word for adequada para executar o Bloco de Notas, o Bloco de Notas será iniciado dentro da sessão existente. Se o Bloco de Notas não puder ser executado a partir da sessão existente — por exemplo, se a restrição de tag excluir a máquina em que a sessão está sendo executada — uma nova sessão em uma máquina adequada será criada em vez de usar o compartilhamento de sessão.

- **Um exemplo em que desabilitar o compartilhamento de sessão entre grupos de aplicativos é útil:**

  Você tem um conjunto de aplicativos que não interagem bem com outros aplicativos instalados nas mesmas máquinas, como duas versões diferentes da mesma suíte de software ou duas versões diferentes do mesmo navegador da web. Você prefere não permitir que um usuário inicie ambas as versões na mesma sessão.

  Você cria um grupo de aplicativos para cada versão da suíte de software e adiciona os aplicativos de cada versão da suíte de software ao grupo de aplicativos correspondente. Se o compartilhamento de sessão entre grupos estiver desabilitado para cada um desses grupos de aplicativos, um usuário especificado nesses grupos poderá executar aplicativos da mesma versão na mesma sessão e ainda poderá executar outros aplicativos ao mesmo tempo, mas não na mesma sessão. Se o usuário iniciar um dos aplicativos de versão diferente (que estão em um grupo de aplicativos diferente) ou iniciar qualquer aplicativo que não esteja contido em um grupo de aplicativos, esse aplicativo será iniciado em uma nova sessão.

Este recurso de compartilhamento de sessão entre grupos de aplicativos não é um recurso de sandboxing de segurança. Não é infalível e não pode impedir que os usuários iniciem aplicativos em suas sessões por outros meios (por exemplo, através do Windows Explorer).

Se uma máquina estiver na capacidade máxima, novas sessões não serão iniciadas nela. Novos aplicativos são iniciados em sessões existentes na máquina, conforme necessário, usando o compartilhamento de sessão (desde que isso esteja em conformidade com as restrições de compartilhamento de sessão descritas aqui).

Você só pode disponibilizar sessões pré-iniciadas para grupos de aplicativos que permitem o compartilhamento de sessão de aplicativos. (As sessões que usam o recurso de permanência de sessão estão disponíveis para todos os grupos de aplicativos.) Esses recursos devem ser

habilitados e configurados em cada um dos grupos de entrega associados ao grupo de aplicativos. Você não pode configurá-los nos grupos de aplicativos.

Por padrão, o compartilhamento de sessão de aplicativo entre grupos de aplicativos é habilitado quando você cria um grupo de aplicativos. Você não pode alterar isso ao criar o grupo. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

Desabilitar o compartilhamento de sessão dentro de um grupo de aplicativos

Você pode impedir o compartilhamento de sessão de aplicativo entre aplicativos que estão no mesmo grupo de aplicativos.

- **Um exemplo de quando desabilitar o compartilhamento de sessão dentro de grupos de aplicativos é útil:**

  Você deseja que seus usuários acessem várias sessões simultâneas em tela cheia de um aplicativo em monitores separados.

  Você cria um grupo de aplicativos e adiciona os aplicativos a ele. Se o compartilhamento de sessão for proibido entre aplicativos nesse grupo de aplicativos, quando um usuário especificado nele iniciar um aplicativo após o outro, eles serão iniciados em sessões separadas, e o usuário poderá mover cada um para um monitor separado.

Por padrão, o compartilhamento de sessão de aplicativo é habilitado quando você cria um grupo de aplicativos. Você não pode alterar isso ao criar o grupo. Depois de criar um grupo de aplicativos, você pode editar o grupo para alterar essa configuração. Consulte Gerenciar grupos de aplicativos.

Criar um grupo de aplicativos

Use o processo de criação de um Grupo de Aplicativos para criar Categorias de Aplicativos no Citrix Workspace™ app. As Categorias de Aplicativos permitem que você gerencie coleções de aplicativos no Citrix Workspace app.

Para criar um grupo de aplicativos:

1. No Studio, selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Para organizar grupos de aplicativos usando pastas, crie pastas sob a pasta raiz **Grupos de Aplicativos**. Para obter mais informações, consulte Organizar grupos de aplicativos usando pastas.

3. Selecione a pasta onde você deseja criar o grupo e clique em **Criar Grupo de Aplicativos**. O assistente de criação de grupo é iniciado com uma página de **Introdução**. Você pode remover a página de futuras inicializações deste assistente.
4. Siga o assistente para configurar as definições nas páginas descritas abaixo. Quando terminar cada página, selecione **Avançar** até chegar à página de **Resumo**.

Etapa 1. Grupos de entrega

A página **Grupos de Entrega** lista todos os grupos de entrega, com o número de máquinas que cada grupo contém.

- A lista **Grupos de Entrega Compatíveis** contém grupos de entrega que você pode selecionar. Grupos de entrega compatíveis contêm máquinas de SO de servidor ou desktop aleatórias (não atribuídas permanentemente ou estaticamente).
- A lista **Grupos de Entrega Incompatíveis** contém grupos de entrega que você não pode selecionar. Cada entrada explica por que não é compatível, como conter máquinas atribuídas estaticamente.

Um grupo de aplicativos pode ser associado a grupos de entrega que contêm máquinas compartilhadas (não privadas) que podem entregar aplicativos.

Você também pode selecionar grupos de entrega que contêm máquinas compartilhadas que entregam apenas desktops, se ambas as seguintes condições forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão do XenDesktop anterior a 7.9.
- Você tem permissão de Editar Grupo de Entrega.

O tipo de grupo de entrega é automaticamente convertido para "desktops e aplicativos" quando o assistente de criação de grupo é confirmado.

Embora você possa criar um grupo de aplicativos que não tenha grupos de entrega associados (talvez para organizar aplicativos ou para servir como armazenamento para aplicativos não utilizados atualmente), o grupo de aplicativos não pode ser usado para entregar aplicativos até que especifique pelo menos um grupo de entrega. Além disso, você não pode adicionar aplicativos ao grupo de aplicativos a partir da origem do menu **Iniciar** se nenhum grupo de entrega for especificado.

Os grupos de entrega que você seleciona especificam as máquinas que serão usadas para entregar aplicativos. Marque as caixas de seleção ao lado dos grupos de entrega que você deseja associar ao grupo de aplicativos.

Para adicionar uma restrição de tag, selecione **Restringir inicializações a máquinas com a tag** e então selecione a tag no menu suspenso.

Etapa 2. Usuários

Especifique quem pode usar os aplicativos no grupo de aplicativos. Você pode permitir que todos os usuários e grupos de usuários nos grupos de entrega selecionados na página anterior usem, ou selecionar usuários e grupos de usuários específicos desses grupos de entrega. Se você restringir o uso aos usuários que especificar, somente os usuários especificados no grupo de entrega e no grupo de aplicativos poderão acessar os aplicativos neste grupo de aplicativos. Essencialmente, a lista de usuários no grupo de aplicativos fornece um filtro para as listas de usuários nos grupos de entrega.

Habilitar ou desabilitar o uso de aplicativos por usuários não autenticados está disponível apenas em grupos de entrega, não em grupos de aplicativos.

Para obter informações sobre onde as listas de usuários são especificadas em uma implantação, consulte Onde as listas de usuários são especificadas.

Etapa 3. Aplicativos

É bom saber:

- Por padrão, os novos aplicativos que você adiciona são colocados em uma pasta chamada **Aplicativos**. Você pode especificar uma pasta diferente. Se você tentar adicionar um aplicativo e um com o mesmo nome já existir nessa pasta, será solicitado que você renomeie o aplicativo que está adicionando. Se você concordar com o nome exclusivo sugerido, o aplicativo será adicionado com esse novo nome. Caso contrário, você deve renomeá-lo antes que possa ser adicionado. Para obter detalhes, consulte Gerenciar pastas de aplicativos.
- Você pode alterar as propriedades (configurações) de um aplicativo ao adicioná-lo ou posteriormente. Consulte Alterar propriedades do aplicativo. Se você publicar dois aplicativos com o mesmo nome para os mesmos usuários, altere a propriedade **Nome do aplicativo (para usuário)** no Studio. Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace.
- Quando você adiciona um aplicativo a mais de um grupo de aplicativos, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para visualizar o aplicativo em todos esses grupos. Nesses casos, consulte um administrador com permissões maiores ou tenha seu escopo estendido para incluir todos os grupos aos quais o aplicativo foi adicionado.

Selecione o menu suspenso **Adicionar** para exibir as fontes do aplicativo.

- **Do menu Iniciar:** Aplicativos que são descobertos em uma máquina nos grupos de entrega selecionados. Ao selecionar esta fonte, uma nova página é aberta com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e, em seguida, selecione **OK**.

  Esta fonte não pode ser selecionada se você selecionou qualquer um dos seguintes:

  - Grupos de aplicativos que não têm grupos de entrega associados.
  - Grupos de aplicativos com grupos de entrega associados que não contêm máquinas.
  - Um grupo de entrega que não contém máquinas.

- **Manualmente:** Aplicativos localizados no site ou em outro lugar da sua rede. Ao selecionar esta fonte, uma nova página é aberta onde você digita o caminho para o executável, diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários. Depois de inserir essas informações, selecione **OK**.
- **Existente**: Aplicativos adicionados anteriormente ao site. Ao selecionar esta origem, uma nova página é iniciada com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e, em seguida, selecione **OK**. Esta origem não pode ser selecionada se o site não tiver aplicativos.
- **Pacotes de aplicativos:** Aplicativos em pacotes de aplicativos App-V, MSIX, MSIX app attach ou FlexApp. Ao selecionar esta origem, a página **Adicionar Aplicativos de Pacotes** é iniciada. Selecione uma origem de pacote de aplicativos, selecione os aplicativos que deseja adicionar na exibição resultante e, em seguida, selecione **OK**.

> **Nota:**
>
> Para publicar aplicativos MSIX ou MSIX app attach, o nível funcional do grupo de entrega deve ser 2106 ou posterior. Para aplicativos FlexApp, o nível funcional deve ser 2206 ou posterior. Quando um requisito de nível funcional não é atendido, as opções correspondentes na lista suspensa **Origem do pacote de aplicativos** ficam esmaecidas. **Nota:**
>
> Na versão 2003 e posterior do VDA, a publicação de pacotes App-V a partir de URLs HTTP não é suportada. Você não pode selecionar esses aplicativos na lista.

Conforme observado, certas entradas no menu suspenso **Adicionar** não serão selecionáveis se não houver uma origem válida desse tipo. As origens incompatíveis não são listadas (por exemplo, você não pode adicionar grupos de aplicativos a grupos de aplicativos, portanto, essa origem não é listada ao criar um grupo de aplicativos).

Etapa 4. Escopos

Esta página aparece somente se você tiver criado anteriormente um escopo personalizado. Por padrão, o escopo **Todos** é selecionado. Para obter mais informações, consulte Administração delegada.

Etapa 5. Resumo

Insira um nome para o grupo de aplicativos. Você também pode (opcionalmente) inserir uma descrição.

Revise as informações de resumo e, em seguida, selecione **Concluir**.

Gerenciar grupos de aplicativos

Introdução

Este artigo descreve como gerenciar os grupos de aplicativos que você criou.

Consulte Aplicativos para obter informações sobre como gerenciar aplicativos em grupos de aplicativos ou grupos de entrega, incluindo como:

- Adicionar ou remover aplicativos em um grupo de aplicativos.
- Alterar associações de grupo de aplicativos.

O gerenciamento de grupos de aplicativos requer as permissões de administração delegada da função interna de Administrador de Grupo de Entrega. Para obter detalhes, consulte Administração delegada.

Habilitar ou desabilitar um grupo de aplicativos

Quando um grupo de aplicativos está habilitado, ele pode entregar os aplicativos que foram adicionados a ele. Desabilitar um grupo de aplicativos desabilita cada aplicativo nesse grupo. No entanto, se esses aplicativos também estiverem associados a outros grupos de aplicativos habilitados, eles poderão ser entregues a partir desses outros grupos. Da mesma forma, se o aplicativo foi explicitamente adicionado a grupos de entrega associados ao grupo de aplicativos

(além de ser adicionado ao grupo de aplicativos), desabilitar o grupo de aplicativos não afeta os aplicativos nesses grupos de entrega.

Um grupo de aplicativos é habilitado quando você o cria. Você não pode alterar isso ao criar o grupo.

1. No Studio, selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Na página **Configurações**, selecione ou desmarque a caixa de seleção **Habilitar Grupo de Aplicativos**.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Habilitar ou desabilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos

O compartilhamento de sessão entre grupos de aplicativos é habilitado quando você cria um grupo de aplicativos. Você não pode alterar isso ao criar o grupo. Para obter mais informações, consulte Compartilhamento de sessão com grupos de aplicativos.

1. No Studio, selecione **Aplicativos** no painel esquerdo e depois selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e depois selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Na página **Configurações**, marque ou desmarque a caixa de seleção **Habilitar compartilhamento de sessão de aplicativo entre Grupos de Aplicativos**.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Desabilitar o compartilhamento de sessão de aplicativo dentro de um grupo de aplicativos

O compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos é habilitado por padrão quando você cria um grupo de aplicativos. Se você desabilitar o compartilhamento de sessão de aplicativo entre grupos de aplicativos, o compartilhamento de sessão entre aplicativos no mesmo grupo de aplicativos permanecerá habilitado.

Você pode usar o SDK do PowerShell para configurar grupos de aplicativos com o compartilhamento de sessão de aplicativo desabilitado entre os aplicativos que eles contêm. Em algumas circunstâncias, isso pode ser desejável. Por exemplo, você pode querer que os usuários iniciem aplicativos não-seamless em janelas de aplicativos em tamanho real em monitores separados.

Quando você desabilita o compartilhamento de sessão de aplicativo dentro de um grupo de aplicativos, cada aplicativo nesse grupo é iniciado em uma nova sessão de aplicativo. Se uma sessão desconectada adequada estiver disponível e estiver executando o mesmo aplicativo, ela será reconectada. Por exemplo, se você iniciar o Bloco de Notas e houver uma sessão desconectada com o Bloco de Notas em execução, essa sessão será reconectada em vez de criar uma nova. Se várias sessões desconectadas adequadas estiverem disponíveis, uma das sessões é escolhida para reconectar, de forma aleatória, mas determinística. Se a situação ocorrer novamente nas mesmas circunstâncias, a mesma sessão será escolhida, mas a sessão não é necessariamente previsível de outra forma.

Você pode usar o SDK do PowerShell para desabilitar o compartilhamento de sessão de aplicativo para todos os aplicativos em um grupo de aplicativos existente, ou para criar um grupo de aplicativos com o compartilhamento de sessão de aplicativo desabilitado.

Exemplos de cmdlets do PowerShell

Para desabilitar o compartilhamento de sessão, use os cmdlets do Broker PowerShell New-BrokerApplicationGroup ou Set-BrokerApplicationGroup com o parâmetro SessionSharingEnabled definido como False e o parâmetro SingleAppPerSession definido como True.

- Por exemplo, para criar um grupo de aplicativos com o compartilhamento de sessão de aplicativo desabilitado para todos os aplicativos no grupo:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- Por exemplo, para desabilitar o compartilhamento de sessão de aplicativo entre todos os aplicativos em um grupo de aplicativos existente:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

Considerações

- Para habilitar a propriedade `SingleAppPerSession`, você deve definir a propriedade `SessionSharingEnabled` como False. As duas propriedades não devem ser habilitadas ao

mesmo tempo. O parâmetro `SessionSharingEnabled` refere-se ao compartilhamento de sessões entre grupos de aplicativos.

- O compartilhamento de sessão de aplicativo funciona apenas para aplicativos associados a grupos de aplicativos, mas não associados a grupos de entrega. Todos os aplicativos associados diretamente a um grupo de entrega compartilham sessões por padrão.
- Se um aplicativo for atribuído a vários grupos de aplicativos, certifique-se de que os grupos não tenham configurações conflitantes. Por exemplo, um grupo com a opção definida como True e a opção de outro grupo definida como False resulta em comportamento imprevisível.

Renomear um grupo de aplicativos

1. No Studio, selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Renomear Grupo de Aplicativos** na barra de ações.
3. Especifique o novo nome exclusivo e, em seguida, selecione **OK**.

Adicionar, remover ou alterar a prioridade das associações de grupo de entrega com um grupo de aplicativos

Um grupo de aplicativos pode ser associado a grupos de entrega contendo máquinas compartilhadas (não privadas) que podem entregar aplicativos.

Você também pode selecionar grupos de entrega contendo máquinas compartilhadas que entregam apenas desktops, se ambas as seguintes condições forem atendidas:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão anterior a 7.9.
- Você tem permissão de Editar Grupo de Entrega.

O tipo de grupo de entrega é automaticamente convertido para "desktops e aplicativos" quando a caixa de diálogo **Editar Grupo de Aplicativos** é confirmada.

1. No Studio, selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Grupos de Entrega**.

4. Para adicionar grupos de entrega, selecione **Adicionar**. Selecione as caixas de seleção dos grupos de entrega disponíveis. (Grupos de entrega incompatíveis não podem ser selecionados.) Ao finalizar suas seleções, selecione **OK**.
5. Para remover grupos de entrega, selecione as caixas de seleção dos grupos que deseja remover e, em seguida, selecione **Remover**. Confirme a exclusão quando solicitado.
6. Para alterar a prioridade dos grupos de entrega, selecione a caixa de seleção do grupo de entrega e, em seguida, selecione **Editar Prioridade**. Insira a prioridade (0 = mais alta) e, em seguida, selecione **OK**.
7. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Adicionar, alterar ou remover uma restrição de tag em um grupo de aplicativos

Adicionar, alterar e remover restrições de tag pode ter efeitos inesperados sobre quais máquinas são consideradas para o lançamento de aplicativos. Revise as considerações e precauções em Tags.

1. No Studio, selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Grupos de Entrega**.
4. Para adicionar uma restrição de tag, selecione **Restringir lançamentos a máquinas com a tag** e, em seguida, selecione a tag no menu.
5. Para alterar ou remover uma restrição de tag, selecione uma tag diferente no menu ou remova a restrição de tag desmarcando **Restringir lançamentos a máquinas com esta tag**.
6. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Adicionar ou remover usuários em um grupo de aplicativos

Para obter informações detalhadas sobre usuários, consulte Criar grupos de aplicativos.

1. No Studio, selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.

2. Selecione um grupo de aplicativos e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Usuários**. Indique se você deseja permitir que todos os usuários nos grupos de entrega associados usem aplicativos no grupo de aplicativos, ou apenas usuários e grupos específicos. Para adicionar usuários, selecione **Adicionar** e, em seguida, especifique os usuários que deseja adicionar. Para remover usuários, selecione um ou mais usuários e, em seguida, selecione **Remover**.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Adicionar, alterar ou remover um ícone de aplicativo em um grupo de aplicativos

Execute as seguintes etapas para adicionar, alterar ou remover um ícone de aplicativo.

1. No painel de navegação, selecione **Aplicativos**.
2. Na guia **Todos os Aplicativos**, selecione um aplicativo e, em seguida, selecione **Propriedades**.

   Para fazer alterações no nível do grupo de aplicativos, navegar até a guia **Grupos de Aplicativos**, selecione um aplicativo em um grupo e, em seguida, selecione **Propriedades**.
3. Selecione a página **Entrega** e, em seguida, selecione **Alterar**. A janela **Selecionar Ícone** é exibida.
4. Na janela **Selecionar Ícone**, faça o seguinte:

   - Para adicionar um ícone, selecione **Adicionar** e, em seguida, navegue até o ícone.
   - Para remover um ícone, selecione-o e, em seguida, selecione **Remover**.
   - Para alterar um ícone, selecione-o para o aplicativo.

> **Importante:**
>
> - Você não pode adicionar um ícone cujo tamanho seja maior que 200 KB.
> - Você pode adicionar apenas arquivos .icon.
> - Você não pode remover ícones incorporados.
> - Você não pode remover um ícone de um aplicativo que está em uso.

5. Selecione **OK** para aplicar as alterações e fechar a janela.

Limitação

- Os ícones padrão para desktops e aplicativos Windows foram alterados para ícones genéricos de desktop de PC para a versão 2209 e posteriores. Essa alteração é aplicável apenas a desktops e aplicativos que apontam para os ícones padrão implantados em versões anteriores a 2209. Se você atualizar para a versão 2209 ou posterior e quiser reverter os ícones para o ícone padrão do aplicativo Windows, execute o seguinte script usando o SDK do PowerShell Remoto:

  ```
  Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0
  ```

Alterar escopos em um grupo de aplicativos

Você pode alterar um escopo somente se tiver criado um escopo (você não pode editar o escopo Todos). Para obter mais informações, consulte Administração delegada.

1. No Studio, selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.
2. Selecione um grupo de aplicativos no painel central e, em seguida, selecione **Editar Grupo de Aplicativos** na barra de ações.
3. Selecione a página **Escopos**. Marque ou desmarque a caixa de seleção ao lado dos escopos que você deseja alterar.
4. Selecione **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou selecione **OK** para aplicar as alterações e fechar a janela.

Excluir um grupo de aplicativos

Um aplicativo deve estar associado a pelo menos um grupo de entrega ou grupo de aplicativos. Se a exclusão de um grupo de aplicativos resultar em um ou mais aplicativos que não pertencem mais a um grupo, você será avisado de que a exclusão desse grupo também excluirá esses aplicativos. Você pode então confirmar ou cancelar a exclusão.

A exclusão de um aplicativo não o exclui de sua fonte original. No entanto, se você quiser torná-lo disponível novamente, deverá adicioná-lo novamente.

1. No Studio, selecione **Aplicativos** no painel esquerdo e, em seguida, selecione a guia **Grupos de Aplicativos**.

2. Selecione um grupo de aplicativos e, em seguida, selecione **Excluir Grupo** na barra de ações.
3. Confirme a exclusão quando solicitado.

Organizar grupos de aplicativos usando pastas

Você pode criar pastas para organizar grupos de aplicativos para facilitar o acesso.

Funções necessárias

Por padrão, você deve ter uma das seguintes funções internas para criar e gerenciar pastas para grupos de aplicativos:

- Administrador da Nuvem
- Administrador Completo
- Administrador de Grupo de Aplicativos

Você pode delegar ações de gerenciamento a outros usuários criando funções personalizadas. A tabela a seguir lista as permissões necessárias para cada ação.

AÇÃO	PERMISSÕES NECESSÁRIAS
Criar pastas de grupo de aplicativos	Criar Pasta de Grupo de Aplicativos
Excluir pastas de grupo de aplicativos	Remover Pasta de Grupo de Aplicativos
Mover pastas de grupo de aplicativos	Mover Pasta de Grupo de Aplicativos
Renomear pastas de grupo de aplicativos	Editar Pasta de Grupo de Aplicativos
Mover grupos de aplicativos para pastas	Editar Pasta de Grupo de Aplicativos, Editar Propriedades do Grupo de Aplicativos

Para obter mais informações, consulte Criar e gerenciar funções.

Criar e gerenciar pastas

Você pode usar a barra de Ações ou o menu de clique com o botão direito para criar e gerenciar pastas de grupo de aplicativos. Além disso, você pode arrastar um grupo de aplicativos ou uma pasta para um local desejado na árvore de pastas.

É bom saber:

- Você pode aninhar pastas em até cinco níveis (*excluindo* a pasta de nó padrão).

- Uma pasta pode conter grupos de aplicativos e subpastas. Você pode excluir uma pasta somente se ela e suas subpastas não contiverem grupos de aplicativos.
- Todos os nós no Studio (como **Catálogos de Máquinas**, **Grupos de Entrega**, **Aplicativos** e **Grupos de Aplicativos**) compartilham a mesma árvore de pastas no back-end. Para evitar conflitos de nomes ao renomear ou mover pastas, use nomes exclusivos para pastas de primeiro nível em diferentes nós.

  Se você criar uma pasta usando o cmdlet SDK `New-BrokerAdminFolder` e quiser que ela apareça sob o nó **Grupos de Aplicativos**, você deve adicionar os metadados `ContainsApplicationGroups` usando o cmdlet `Set-BrokerAdminFolderMetadata`.

  Exemplo:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplicationGroups -Value true
  ```

Acesso Remoto a PC

Nota:

Este artigo descreve como configurar o Acesso Remoto a PC usando o Studio. Se você estiver usando a interface de Implantação Rápida, siga as orientações em Acesso Remoto a PC na Implantação Rápida.

O Acesso Remoto a PC é um recurso do Citrix Virtual Apps and Desktops™ que permite às organizações permitir facilmente que seus funcionários acessem recursos corporativos remotamente de forma segura. A plataforma Citrix torna esse acesso seguro possível, dando aos usuários acesso aos seus PCs físicos de escritório. Se os usuários puderem acessar seus PCs de escritório, eles poderão acessar todos os aplicativos, dados e recursos de que precisam para realizar seu trabalho. O Acesso Remoto a PC elimina a necessidade de introduzir e fornecer outras ferramentas para acomodar o teletrabalho. Por exemplo, desktops ou aplicativos virtuais e sua infraestrutura associada.

O Acesso Remoto a PC usa os mesmos componentes do Citrix Virtual Apps and Desktops que fornecem desktops e aplicativos virtuais. Como resultado, os requisitos e o processo de implantação e configuração do Acesso Remoto a PC são os mesmos exigidos para a implantação do Citrix Virtual Apps and Desktops para a entrega de recursos virtuais. Essa uniformidade

proporciona uma experiência administrativa consistente e unificada. Os usuários recebem a melhor experiência de usuário usando o Citrix HDX para entregar sua sessão de PC de escritório.

O recurso consiste em um catálogo de máquinas do tipo **Acesso Remoto a PC** que oferece a seguinte funcionalidade:

- Capacidade de adicionar máquinas especificando UOs. Essa capacidade facilita a adição de PCs em massa.
- Capacidade de adicionar máquinas usando arquivos CSV. Essa capacidade facilita a adição de PCs em massa em cenários com restrições de estrutura de UO.
- Atribuição automática de usuário com base no usuário que faz login no PC Windows do escritório. Oferecemos suporte a atribuições de usuário único e múltiplos usuários. Por padrão, o Citrix DaaS™ atribui automaticamente vários usuários à próxima máquina não atribuída. Para restringir a atribuição automática a um único usuário, navegar para **Configurações > Configurações do site** e desative a configuração **Habilitar atribuição automática de múltiplos usuários para Acesso Remoto a PC**.

O Citrix Virtual Apps and Desktops pode acomodar mais casos de uso para PCs físicos usando outros tipos de catálogos de máquinas. Esses casos de uso incluem:

- PCs Linux Físicos
- PCs físicos agrupados (ou seja, atribuídos aleatoriamente, não dedicados)

> **Notas:**

> Para obter detalhes sobre as versões de SO suportadas, consulte os requisitos de sistema para o VDA para SO de sessão única e VDA Linux.

> Para implantações locais, o Acesso Remoto a PC é válido apenas para licenças Citrix DaaS Advanced ou Premium. As sessões consomem licenças da mesma forma que outras sessões do Citrix Virtual Desktops™. Para o Citrix Cloud, o Acesso Remoto a PC é válido para Citrix DaaS e Workspace Premium Plus.

Considerações

Embora todos os requisitos técnicos e considerações que se aplicam ao Citrix Virtual Apps and Desktops e ao Citrix DaaS em geral também se apliquem ao Acesso Remoto a PC, alguns podem ser mais relevantes ou exclusivos para o caso de uso de PC físico.

Importante:

Sistemas físicos com Windows 11 (e alguns com Windows 10) incluem recursos de segurança baseados em virtualização que fazem com que o software VDA os detecte incorretamente como máquinas virtuais. Para mitigar esse problema, você tem as seguintes opções:

- Use a opção "/physicalmachine" juntamente com a opção "/remotepc" como parte da instalação do VDA por linha de comando
- Adicione o seguinte valor de registro após a instalação do VDA, caso a opção mencionada não tenha sido usada `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - Nome: ForceEnableRemotePC
  - Tipo: DWORD
  - Dados: 1

Considerações de implantação

Ao planejar a implantação do Acesso Remoto a PC, tome algumas decisões gerais.

- Você pode adicionar o Acesso Remoto a PC a uma implantação existente do Citrix Virtual Apps and Desktops e do Citrix DaaS. Antes de escolher esta opção, considere o seguinte:
  - Os Delivery Controllers ou Cloud Connectors atuais estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs de Acesso Remoto a PC?
  - Os bancos de dados do site on-premises e os servidores de banco de dados estão dimensionados adequadamente para suportar a carga adicional associada aos VDAs de Acesso Remoto a PC?
  - Os VDAs existentes e os novos VDAs de Acesso Remoto a PC excederão o número máximo de VDAs suportados por site?
- Você deve implantar o VDA em PCs de escritório por meio de um processo automatizado. As seguintes são duas das opções disponíveis:
  - Ferramentas de Distribuição Eletrônica de Software (ESD), como SCCM: Instalar VDAs usando SCCM.

    - Scripts de implantação: Instalar VDAs usando scripts.

- Revise as considerações de segurança do Acesso Remoto a PC.

Considerações sobre o catálogo de máquinas

O tipo de catálogo de máquinas necessário depende do caso de uso:

- Catálogo de máquinas de Acesso Remoto a PC
    - PCs dedicados Windows/Linux
    - PCs multiusuário dedicados Windows/Linux. Este caso de uso se aplica a PCs físicos de escritório que vários usuários podem acessar remotamente em diferentes turnos.
    - PCs Windows/Linux agrupados. Este caso de uso se aplica a PCs físicos que vários usuários aleatórios podem acessar, como laboratórios de informática.

Depois de identificar o tipo de catálogo de máquinas, considere o seguinte:

- Uma máquina pode ser atribuída a apenas um catálogo de máquinas por vez.
- Para facilitar a administração delegada, considere criar catálogos de máquinas com base na localização geográfica, departamento ou qualquer outro agrupamento que facilite a delegação da administração de cada catálogo aos administradores apropriados.
- Ao escolher as UOs nas quais as contas de máquina residem, selecione UOs de nível inferior para maior granularidade. Se tal granularidade não for necessária, você pode escolher UOs de nível superior. Por exemplo, no caso de Banco/Oficiais/Caixas, selecione **Caixas** para maior granularidade. Caso contrário, você pode selecionar **Oficiais** ou **Banco** com base no requisito.
- Mover ou excluir UOs depois de serem atribuídas a um catálogo de máquinas de Acesso Remoto a PC afeta as associações de VDA e causa problemas com atribuições futuras. Portanto, certifique-se de planejar adequadamente para que as atualizações de atribuição de UO para catálogos de máquinas sejam consideradas no plano de alteração do Active Directory.
- Você pode escolher UOs para adicionar máquinas ao catálogo de máquinas em massa. Em alguns cenários, fazer isso não é fácil devido a restrições de estrutura de UO. Em vez disso, você pode adicionar máquinas em massa usando arquivos CSV. Esse recurso oferece mais flexibilidade para adicionar máquinas em massa. Você pode adicionar apenas máquinas (para uso com atribuições automáticas de usuário) ou adicionar máquinas junto com atribuições de usuário.
- O Wake on LAN integrado está disponível apenas com o catálogo de máquinas do tipo **Acesso Remoto a PC**.

Considerações sobre o VDA Linux

Estas considerações são específicas para o VDA Linux:

- O Escurecimento do monitor físico para VDAs de Acesso Remoto a PC está disponível, mas não para todas as distribuições Linux. Para as distribuições Linux não suportadas, use o VDA Linux em máquinas físicas apenas no modo não 3D. Caso contrário, devido a limitações no driver da NVIDIA, a tela local do PC não pode ser escurecida e exibe as atividades da sessão quando o modo HDX 3D está ativado. Mostrar esta tela é um risco de segurança.
- Recomendamos que você use catálogos de máquinas do tipo SO de sessão única para máquinas Linux físicas.

Requisitos técnicos e considerações

Esta seção contém os requisitos técnicos e considerações para PCs físicos.

- O seguinte não é suportado:
  - Comutadores KVM ou outros componentes que podem desconectar uma sessão.
  - PCs híbridos, incluindo laptops e PCs All-in-One e NVIDIA Optimus.
  - Máquinas com dual boot.
- Conecte o teclado e o mouse diretamente ao PC. A conexão a um monitor ou outros componentes que podem ser desligados ou desconectados pode tornar esses periféricos indisponíveis. Se você precisar conectar os dispositivos de entrada a componentes como monitores, não desligue esses componentes.
- Os PCs devem estar ingressados em um domínio do Active Directory Domain Services.
- O Secure Boot é suportado apenas no Windows 10.
- O PC deve ter uma conexão de rede ativa. Uma conexão com fio é preferível para maior confiabilidade e largura de banda.
- Se estiver usando Wi-Fi, faça o seguinte:
  a. Defina as configurações de energia para manter o adaptador sem fio ligado.
  b. Configure o adaptador sem fio e o perfil de rede para permitir a conexão automática à rede sem fio antes que o usuário faça logon. Caso contrário, o VDA não se registrará até que o usuário faça logon. O PC não estará disponível para acesso remoto até que um usuário tenha feito logon.
  c. Certifique-se de que os Delivery Controllers ou Cloud Connectors possam ser alcançados a partir da rede Wi-Fi.

- Você pode usar o Acesso Remoto ao PC em computadores laptop. Certifique-se de que o laptop esteja conectado a uma fonte de energia em vez de funcionar com a bateria. Configure as opções de energia do laptop para corresponder às opções de um PC desktop. Por exemplo:

  a. Desative o recurso de hibernação.

  b. Desative o recurso de suspensão.

  c. Defina a ação de fechar a tampa como **Não fazer nada**.

  d. Defina a ação de "pressionar o botão liga/desliga" como **Desligar**.

  e. Desative os recursos de economia de energia da placa de vídeo e da NIC.

- O Acesso Remoto ao PC é compatível com dispositivos Surface Pro com Windows 10. Siga as mesmas diretrizes para laptops mencionadas anteriormente.
- Se estiver usando uma estação de acoplamento, você pode desacoplar e reacoplar laptops. Ao desacoplar o laptop, o VDA se registra novamente com os Delivery Controllers ou Cloud Connectors via Wi-Fi. No entanto, ao reacoplar o laptop, o VDA não muda para usar a conexão com fio, a menos que você desconecte o adaptador sem fio. Alguns dispositivos fornecem funcionalidade integrada para desconectar o adaptador sem fio ao estabelecer uma conexão com fio. Os outros dispositivos exigem soluções personalizadas ou utilitários de terceiros para desconectar o adaptador sem fio. Revise as considerações sobre Wi-Fi mencionadas anteriormente.

  Faça o seguinte para habilitar o acoplamento e desacoplamento para dispositivos de Acesso Remoto ao PC:

  a. No menu **Iniciar**, selecione **Configurações > Sistema > Energia e suspensão** e defina **Suspender** como **Nunca**.

  b. Em **Gerenciador de Dispositivos > Adaptadores de rede > Adaptador Ethernet**, vá para **Gerenciamento de Energia** e desmarque **Permitir que o computador desligue este dispositivo para economizar energia**. Certifique-se de que **Permitir que este dispositivo reative o computador** esteja marcado.

- Vários usuários com acesso ao mesmo PC de escritório veem o mesmo ícone no aplicativo Citrix Workspace. Quando um usuário faz logon no aplicativo Citrix Workspace, esse recurso aparece como indisponível se já estiver em uso por outro usuário.
- Instale o aplicativo Citrix Workspace em cada dispositivo cliente (por exemplo, um PC doméstico) que acessa o PC do escritório.

Sequência de configuração

Esta seção contém uma visão geral de como configurar o Acesso Remoto ao PC ao usar o catálogo de máquinas do tipo **Acesso Remoto ao PC**. Para obter informações sobre como criar outros tipos de catálogos de máquinas, consulte Criar catálogos de máquinas.

1. Somente site local - Para usar o recurso integrado Wake on LAN, configure os pré-requisitos descritos em Wake on LAN.
2. Se um novo site do Citrix Virtual Apps and Desktops foi criado para Acesso Remoto ao PC:

    a. Selecione o tipo de site **Acesso Remoto ao PC**.

    b. Na página **Gerenciamento de Energia**, escolha habilitar ou desabilitar o gerenciamento de energia para o catálogo de máquinas padrão de Acesso Remoto ao PC. Você pode alterar essa configuração posteriormente editando as propriedades do catálogo de máquinas. Para obter detalhes sobre como configurar o Wake on LAN, consulte Wake on LAN.

    c. Preencha as informações nas páginas **Usuários** e **Contas de Máquina**.

    A conclusão dessas etapas cria um catálogo de máquinas chamado **Máquinas de Acesso Remoto ao PC** e um grupo de entrega chamado **Desktops de Acesso Remoto ao PC**.
3. Se estiver adicionando a um site existente do Citrix Virtual Apps and Desktops:

    a. Crie um catálogo de máquinas do tipo **Acesso Remoto ao PC** (página Sistema Operacional do assistente). Para obter detalhes sobre como criar um catálogo de máquinas, consulte Criar catálogos de máquinas. Certifique-se de atribuir a OU correta para que os PCs de destino fiquem disponíveis para uso com o Acesso Remoto ao PC.

    b. Crie um grupo de entrega para fornecer aos usuários acesso aos PCs no catálogo de máquinas. Para obter detalhes sobre como criar um grupo de entrega, consulte Criar grupos de entrega. Certifique-se de atribuir o grupo de entrega a um grupo do Active Directory que contenha os usuários que precisam de acesso aos seus PCs.
4. Implante o VDA nos PCs do escritório.

    - Recomendamos usar o instalador VDA principal do SO de sessão única (`VDAWorkstationCoreSetup.exe`).
    - Você também pode usar o instalador VDA completo de sessão única (`VDAWorkstationSetup.exe`) com a opção `/remotepc /physicalmachine`, que alcança o mesmo resultado que usar o instalador VDA principal.

- Considere habilitar a Assistência Remota do Windows para permitir que as equipes de suporte técnico forneçam suporte remoto através do Citrix Director. Para fazer isso, use a opção `/enable_remote_assistance`. Para obter detalhes, consulte Instalar usando a linha de comando.
- Para poder ver as informações de duração de logon no Director, você deve usar o instalador VDA completo de sessão única e incluir o componente **Citrix User Profile Management WMI Plugin**. Inclua este componente usando a opção `/includeadditional`. Para obter detalhes, consulte Instalar usando a linha de comando.
- Para obter informações sobre como implantar o VDA usando o SCCM, consulte Instalar VDAs usando o SCCM.
- Para obter informações sobre como implantar o VDA por meio de scripts de implantação, consulte Instalar VDAs usando scripts.

Depois de concluir com sucesso as etapas 2 a 4, os usuários são automaticamente atribuídos às suas próprias máquinas quando fazem login localmente nos PCs.

5. Instrua os usuários a baixar e instalar o aplicativo Citrix Workspace em cada dispositivo cliente que eles usam para acessar o PC do escritório remotamente. O aplicativo Citrix Workspace está disponível no site de download da Citrix ou nas lojas de aplicativos para dispositivos móveis compatíveis.

Recursos gerenciados através do registro

> **Cuidado:**
>
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Modo de suspensão (versão mínima 7.16)

Para permitir que uma máquina de Acesso Remoto a PC entre em estado de suspensão, adicione esta configuração de registro no VDA e, em seguida, reinicie a máquina. Após a reinicialização, as configurações de economia de energia do sistema operacional são respeitadas. A máquina entra em modo de suspensão após o tempo limite de inatividade pré-configurado. Depois que a máquina acorda, ela se registra novamente com o Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Valor: 1

Gerenciamento de sessão

Por padrão, a sessão de um usuário remoto é automaticamente desconectada quando um usuário local inicia uma sessão nessa máquina (pressionando CTRL+ALT+DEL). Para evitar essa ação automática, adicione a seguinte entrada de registro no PC do escritório e, em seguida, reinicie a máquina.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: SasNotification
- Tipo: DWORD
- Valor: 1

Por padrão, o usuário remoto tem preferência sobre o usuário local quando a mensagem de conexão não é reconhecida dentro do período de tempo limite. Para configurar o comportamento, use esta configuração:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaMode
- Tipo: DWORD
- Valor:
  - 1 - O usuário remoto sempre tem preferência se ele ou ela não responder à interface de mensagens no período de tempo limite especificado. Este comportamento é o padrão se esta configuração não for definida.
  - 2 - O usuário local tem preferência.

O tempo limite para aplicar o modo Acesso Remoto ao PC é de 30 segundos por padrão. Você pode configurar esse tempo limite, mas não o defina para menos de 30 segundos. Para configurar o tempo limite, use esta configuração de registro:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nome: RpcaTimeout

- Tipo: DWORD
- Dados: número de segundos para o tempo limite em valores decimais

Quando um usuário deseja obter acesso forçado ao console: O usuário local pode pressionar Ctrl+Alt+Del duas vezes em um intervalo de 10 segundos para obter controle local sobre uma sessão remota e forçar um evento de desconexão.

Após a alteração do registro e a reinicialização da máquina, se um usuário local pressionar Ctrl+Alt+Del para fazer logon nesse PC enquanto ele estiver em uso por um usuário remoto, o usuário remoto receberá um prompt. O prompt pergunta se deve permitir ou negar a conexão do usuário local. Permitir a conexão desconecta a sessão do usuário remoto.

Wake on LAN

O Acesso Remoto ao PC suporta Wake on LAN, o que oferece aos usuários a capacidade de ligar PCs físicos remotamente. Esse recurso permite que os usuários mantenham seus PCs de escritório desligados quando não estiverem em uso para economizar custos de energia. Ele também permite o acesso remoto quando uma máquina foi desligada inadvertidamente.

Com o recurso Wake on LAN, os pacotes mágicos são enviados diretamente do VDA em execução no PC para a sub-rede na qual o PC reside, quando instruído pelo controlador de entrega. Isso permite que o recurso funcione sem dependências de componentes de infraestrutura adicionais ou soluções de terceiros para a entrega de pacotes mágicos.

O recurso Wake on LAN difere do recurso Wake on LAN herdado baseado em SCCM. O Wake on LAN integrado ao SCCM é uma opção alternativa de Wake on LAN para Acesso Remoto ao PC que está disponível apenas com Citrix Virtual Apps and Desktops locais. Para obter informações sobre o Wake on LAN baseado em SCCM, consulte Wake on LAN – SCCM-integrated.

Limitação

O Acesso Remoto ao PC com o recurso Wake on LAN não suporta o ligamento automático durante os horários de pico.

Requisitos do sistema

A seguir estão os requisitos do sistema para usar o recurso Wake on LAN:

- Plano de controle:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 ou posterior

- PCs físicos:
  - VDA versão 2009 ou posterior
  - Windows 10 ou Windows 11. Para obter detalhes de compatibilidade, consulte os requisitos de sistema do VDA.
  - Wake on LAN ativado na BIOS/UEFI
  - Wake on LAN ativado nas propriedades do adaptador de rede na configuração do Windows

Configurar Wake on LAN

Para configurar o Wake on LAN, você pode usar o Studio ou o PowerShell.

Configurar Wake on LAN usando o Studio

Para criar a conexão Wake on LAN:

1. navegar até o nó **Hospedagem** à esquerda.
2. Selecione **Adicionar Conexão e Recursos**.
3. Na página **Conexão** do assistente, forneça o seguinte:
   a. Tipo de conexão: Wake on LAN de PC Remoto
   b. Nome da zona: selecione a zona onde reside o catálogo do Acesso Remoto para PC
   c. Nome da conexão: insira um nome para a conexão Wake on LAN
4. Finalize as etapas restantes no assistente Adicionar Conexão e Recursos.

Para adicionar a conexão Wake on LAN a um catálogo de máquinas de Acesso Remoto para PC:

1. Se você estiver criando um novo catálogo de máquinas de Acesso Remoto para PC, poderá adicionar a conexão na página **Tipo de Máquina** do assistente de Configuração do Catálogo de Máquinas usando a lista suspensa.
2. Se você quiser adicionar a conexão Wake on LAN a um catálogo de máquinas existente:
   a. navegar até o nó **Catálogos de Máquinas** à esquerda.
   b. Selecione o catálogo de máquinas de Acesso Remoto para PC apropriado.
   c. Clique com o botão direito do mouse no catálogo de máquinas ou selecione o menu **Mais** acima.
   d. Selecione **Editar Catálogo de Máquinas**.
   e. Na página **Gerenciamento de Energia**, selecione **Sim**.

f. Selecione a conexão apropriada na lista suspensa.

g. Selecione **Salvar**.

> **Nota:**
>
> A configuração de Wake on LAN através do Studio está disponível apenas com o Citrix DaaS neste momento.

Configurar Wake on LAN usando PowerShell

Para configurar o Wake on LAN usando PowerShell:

1. Crie o catálogo de máquinas do Acesso Remoto ao PC se você ainda não tiver um.
2. Crie a conexão de host do Wake on LAN se você ainda não tiver uma.
3. Recupere o identificador exclusivo da conexão de host do Wake on LAN.
4. Associe a conexão de host do Wake on LAN a um catálogo de máquinas.

Para criar a conexão de host do Wake on LAN:

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `
```

```
                -Password "wolpwd" `

                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

Quando a conexão de host estiver pronta, execute os seguintes comandos para recuperar o identificador exclusivo da conexão de host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

Depois de recuperar o identificador exclusivo da conexão, execute os seguintes comandos para associar a conexão ao catálogo de máquinas do Acesso Remoto ao PC:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

Considerações de design

Ao planejar usar o Wake on LAN com o Acesso Remoto ao PC, considere o seguinte:

- Vários catálogos de máquinas podem usar a mesma conexão de host do Wake on LAN.
- Para que um PC ative outro PC, ambos os PCs devem estar na mesma sub-rede e usar a mesma conexão de host do Wake on LAN. Não importa se os PCs estão no mesmo catálogo de máquinas ou em catálogos diferentes.
- As conexões de host são atribuídas a zonas específicas. Se sua implantação contiver mais de uma zona, você precisará de uma conexão de host do Wake on LAN em cada zona. O mesmo se aplica aos catálogos de máquinas.
- Pacotes mágicos são transmitidos usando o endereço de broadcast global 255.255.255.255. Certifique-se de que o endereço não esteja bloqueado.
- Deve haver pelo menos um PC ligado na sub-rede — para cada conexão Wake on LAN — para poder ativar máquinas nessa sub-rede.

Considerações operacionais

A seguir estão as considerações para usar o recurso Wake on LAN:

- O VDA deve se registrar pelo menos uma vez antes que o PC possa ser ativado usando o recurso integrado Wake on LAN.
- O Wake on LAN só pode ser usado para ativar PCs. Ele não oferece suporte a outras ações de energia, como reiniciar ou desligar.
- Pacotes mágicos são enviados de uma das duas maneiras:
  a. Quando um usuário tenta iniciar uma sessão em seu PC e o VDA está não registrado
  b. Quando um administrador envia manualmente um comando de ligar do Studio ou PowerShell
- Como o Delivery Controller não tem conhecimento do estado de energia de um PC, o Studio exibe **Não Suportado** em estado de energia. O Delivery Controller usa o estado de registro do VDA para determinar se um PC está ligado ou desligado.

Solução de problemas

Escurecimento do monitor não funciona

Se o monitor local do PC Windows não estiver em branco enquanto houver uma sessão HDX™ ativa (o monitor local exibe o que está acontecendo na sessão), é provável que seja devido a problemas com o driver do fornecedor da GPU. Para resolver o problema, dê ao driver de exibição indireta (IDD) da Citrix uma prioridade maior do que o driver do fornecedor da placa gráfica, definindo o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nome: CitrixIDD
- Tipo: DWORD
- Dados: 3

Para mais detalhes sobre as prioridades do adaptador de vídeo e a criação de monitores, consulte o artigo do Knowledge Center CTX237608.

A sessão se desconecta quando você seleciona Ctrl+Alt+Del na máquina que tem a notificação de gerenciamento de sessão habilitada

A notificação de gerenciamento de sessão controlada pelo valor de registro **SasNotification** só funciona quando o modo Acesso Remoto para PC está habilitado no VDA. Se o PC físico tiver a função Hyper-V ou quaisquer recursos de segurança baseados em virtualização habilitados, o PC será relatado como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desabilitará automaticamente o modo Acesso Remoto para PC. Para habilitar o modo Acesso Remoto para PC, adicione o seguinte valor de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

Informações de diagnóstico

As informações de diagnóstico sobre o Acesso Remoto para PC são gravadas no log de Eventos de Aplicativo do Windows. As mensagens informativas não são limitadas. As mensagens de erro são limitadas descartando mensagens duplicadas.

- 3300 (informativo): Máquina adicionada ao catálogo
- 3301 (informativo): Máquina adicionada ao grupo de entrega
- 3302 (informativo): Máquina atribuída ao usuário
- 3303 (erro): Exceção

Gerenciamento de energia

Se o gerenciamento de energia para Acesso Remoto ao PC estiver ativado, as transmissões direcionadas à sub-rede podem falhar ao iniciar máquinas que estão em uma sub-rede diferente do Controller. Se você precisar de gerenciamento de energia entre sub-redes usando transmissões direcionadas à sub-rede, e o suporte AMT não estiver disponível, tente o proxy Wake-up ou o método Unicast. Certifique-se de que essas configurações estejam ativadas nas propriedades avançadas para a conexão de gerenciamento de energia.

A sessão remota ativa registra a entrada local da tela de toque

Quando o VDA ativa o modo de Acesso Remoto ao PC, a máquina ignora a entrada local da tela de toque durante uma sessão ativa. Se o PC físico tiver a função Hyper-V ou quaisquer recursos de segurança baseados em virtualização ativados, o PC se reporta como uma máquina virtual. Se o VDA detectar que está sendo executado em uma máquina virtual, ele desativa automaticamente o modo de Acesso Remoto ao PC. Para ativar o modo de Acesso Remoto ao PC, adicione a seguinte configuração de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nome: ForceEnableRemotePC
- Tipo: DWORD
- Dados: 1

Reinicie o PC para que a configuração entre em vigor.

Mais recursos

A seguir estão outros recursos para Acesso Remoto ao PC:

- Orientação de design da solução: Remote PC Access Design Decisions.
- Exemplos de arquiteturas de Acesso Remoto ao PC: Reference Architecture for Citrix Remote PC Access Solution.

Serviço autônomo da Citrix Secure Ticketing Authority (STA)

O serviço autônomo da Citrix Secure Ticketing Authority (STA) permite que você tenha mais controle sobre a entrega de tickets STA em seu ambiente.

O serviço STA autônomo da Citrix é instalado em cada Cloud Connector em um Local de Recurso por padrão. Este serviço transfere a emissão de tickets STA do serviço de emissão de tickets do Citrix Cloud™ para os Cloud Connectors e padroniza as operações de emissão de tickets nos modos normal e LHC. O serviço STA autônomo reduz a dependência de serviços em nuvem e diminui eventos LHC intermitentes.

Cenários e requisitos de configuração do serviço STA autônomo

O serviço STA autônomo funciona nos modos normal e LHC quando você está usando o seguinte:

- Citrix® StoreFront Cloud com Gateway Local: Os NetScaler® Gateways locais são configurados para proxy HDX por Local de Recurso. Todos os Cloud Connectors em todos os Locais de Recurso para os quais o NetScaler atua como proxy HDX devem ser listados como servidores STA no servidor virtual do NetScaler Gateway. Se alguns servidores STA no Local de Recurso estiverem ausentes, os lançamentos poderão falhar.
- StoreFront™ com Gateway Local: Todos os Cloud Connectors listados como servidores STA no servidor StoreFront devem ser listados como servidores STA no servidor virtual do NetScaler Gateway. Se alguns dos Cloud Connectors listados no StoreFront não estiverem listados no servidor virtual do NetScaler Gateway, os lançamentos poderão falhar.

Remover componentes

Para remover componentes que você instalou (como VDAs), a Citrix® recomenda usar o recurso do Windows para remover ou alterar programas. Alternativamente, você pode remover componentes usando a linha de comando ou um script.

Ao remover componentes, os pré-requisitos não são removidos e as configurações do firewall não são alteradas.

Ao remover um VDA, a máquina é reiniciada automaticamente após a remoção, por padrão.

Remover componentes usando o recurso do Windows para remover ou alterar programas

No recurso do Windows para remover ou alterar programas:

- Para remover um VDA, selecione **Citrix Virtual Delivery Agent** \<*versão*>, clique com o botão direito e selecione **Desinstalar**. O instalador será iniciado e você poderá selecionar os componentes a serem removidos.
- Para remover o Universal Print Server, selecione **Citrix Universal™ Print Server**, clique com o botão direito e selecione **Desinstalar**.

Remover um VDA usando a linha de comando

Execute o comando que foi usado para instalar o VDA: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` ou `VDAWorkstationCoreSetup.exe`. Consulte Instalar usando a linha de comando para descrições de sintaxe.

- Para remover apenas o VDA ou apenas o aplicativo Citrix Workspace, use as opções `/remove` e `/components`.
- Para remover o VDA e o aplicativo Citrix Workspace, use a opção `/removeall`.

Por exemplo, o comando a seguir remove o VDA e o aplicativo Citrix Workspace™ de uma máquina com SO multissessão.

```
VDAServerSetup.exe /removeall
```

Por exemplo, o comando a seguir remove o VDA, mas não o aplicativo Citrix Workspace para Windows (se estiver instalado) de uma máquina com SO de sessão única.

```
VDAWorkstationSetup.exe /remove /components vda
```

Você também pode remover um VDA usando um script fornecido pela Citrix. Consulte Remover VDAs usando o script.

Camada de personalização do usuário

O recurso de camada de personalização do usuário para Citrix Virtual Apps and Desktops™ estende os recursos de catálogos de máquinas não persistentes para preservar os dados dos usuários e os aplicativos instalados localmente entre as sessões. Alimentado pela tecnologia subjacente do Citrix App Layering, o recurso de camada de personalização do usuário oferece suporte ao Citrix Provisioning e aos Machine Creation Services (MCS) em um catálogo de máquinas não persistente.

Você instala os componentes da camada de personalização do usuário junto com o Virtual Delivery Agent dentro da imagem mestre. Um arquivo VHD armazena aplicativos instalados

localmente pelo usuário. O VHD montado na imagem atua como o próprio disco rígido virtual do usuário.

> **Importante:**

> Você pode implantar camadas de personalização do usuário no Citrix Virtual Apps and Desktops, ou camadas de usuário do App Layering habilitadas em um modelo de imagem, mas não ambos. Não instale o recurso de camada de personalização do usuário em uma camada dentro do App Layering.

> Este recurso substitui o Personal vDisk (PvD), ao mesmo tempo em que oferece uma experiência de espaço de trabalho persistente para usuários em um ambiente de desktop não persistente e agrupado.

Para implantar o recurso de camada de personalização do usuário, instale-o e configure-o usando as etapas detalhadas no artigo. Até então, o recurso não estará disponível.

Suporte a aplicativos

Com exceção das seguintes exceções, todos os aplicativos que um usuário instala localmente na área de trabalho são suportados na camada de personalização do usuário.

Exceções

Os seguintes aplicativos são a exceção e não são suportados na camada de personalização do usuário:

- Aplicativos corporativos, como MS Office e Visual Studio.
- Aplicativos que modificam a pilha de rede ou hardware. Exemplo: um cliente VPN.
- Aplicativos que possuem drivers de nível de inicialização. Exemplo: um verificador de vírus.
- Aplicativos com drivers que usam o armazenamento de drivers. Exemplo: um driver de impressora.

> **Nota:**

> Você pode disponibilizar impressoras usando Objetos de Política de Grupo (GPOs) do Windows.

Não *permita* que os usuários instalem aplicativos não suportados localmente. Em vez disso, instale esses aplicativos diretamente na imagem mestre.

Aplicativos que exigem uma conta de usuário local ou de administrador

Quando um usuário instala um aplicativo localmente, o aplicativo vai para a sua camada de usuário. Se o usuário adicionar ou editar um usuário ou grupo local, as alterações não persistem além da sessão.

> **Importante:**
>
> Adicione qualquer usuário ou grupo local necessário na imagem mestre.

Requisitos

O recurso de camada de personalização do usuário requer os seguintes componentes:

- Citrix Virtual Apps and Desktops 7 1909 ou posterior
- Virtual Delivery Agent (VDA), versão 1912 ou posterior
- Citrix Provisioning™, versão 1909 ou posterior
- Compartilhamento de Arquivos do Windows (SMB), ou Azure Files com autenticação AD local habilitada

Você pode implantar o recurso de camada de personalização do usuário nas seguintes versões do Windows quando o SO é implantado como sessão única. O suporte é limitado a um único usuário em uma única sessão.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, versão 1607 ou posterior
- Windows 10 Multi-Session (Azure Files compatível)
- Windows Server 2016 (Azure Files compatível)
- Windows Server 2019 (Azure Files compatível)

Para Citrix Virtual Apps and Desktops 7, o uso de Azure Files com camadas de personalização de usuário é compatível com Windows Server 2019, Windows Server 2016v e cliente Windows 10.

> **Nota:**

> Se você estiver usando um SO de servidor, apenas o Server VDI é compatível. Para obter detalhes de implantação, consulte o artigo Server VDI.

> A camada de personalização do usuário suporta apenas um usuário por vez por máquina, e então a máquina precisa ser reiniciada para redefinir os discos. Você não pode usar a camada de personalização do usuário com sistemas operacionais de servidor multi-sessão, apenas com sistemas de servidor de sessão única. A camada de personalização do usuário funciona apenas com desktops não persistentes.

> Desinstale o recurso de camada de personalização do usuário, se instalado. Reinicie a imagem mestre antes de instalar a versão mais recente.

Configure seu compartilhamento de arquivos

O recurso de camada de personalização do usuário requer armazenamento Windows Server Message Block (SMB). Para criar um compartilhamento de arquivos do Windows, siga as etapas usuais para o sistema operacional Windows que você está usando.

Para saber mais sobre como usar o Azure Files com catálogos baseados em Azure, consulte Configurar o armazenamento do Azure Files para camadas de personalização do usuário.

Recomendações

Siga as recomendações nesta seção para uma implantação bem-sucedida da camada de personalização do usuário.

Microsoft System Center Configuration Manager (SCCM)

Se você estiver usando o SCCM com o recurso de camada de personalização do usuário, siga as diretrizes da Microsoft para preparar sua imagem em um ambiente VDI. Consulte este artigo do Microsoft TechNet para obter mais informações.

Tamanho da camada de usuário

Uma camada de usuário é um disco com provisionamento dinâmico que se expande à medida que o espaço no disco é usado. O tamanho padrão permitido para uma camada de usuário é de 10 GB, o mínimo que recomendamos.

> **Nota:**

> Durante a instalação, se o valor for definido como zero (0), o tamanho padrão da camada de usuário será definido como 10 GB.

> Se você quiser alterar o tamanho da camada de usuário, poderá inserir um valor diferente para a política do Studio **User Layer Size**. Consulte **Etapa 5: Criar políticas personalizadas de grupo de entrega**, em **Opcional: Clique em Selecionar ao lado de User Layer Size in GB.**

Ferramentas para substituir o tamanho da camada de usuário (Opcional)

Você pode substituir o tamanho da camada de usuário usando uma ferramenta do Windows para definir uma cota no compartilhamento de arquivos da camada de usuário.

Use uma das seguintes ferramentas de cota da Microsoft para definir uma cota rígida no diretório da camada de usuário chamado **Users**:

- Gerenciador de Recursos do Servidor de Arquivos (FSRM)
- Gerenciador de Cotas

> **Nota:**

> Aumentar a cota afeta novas camadas de usuário e expande as existentes. Diminuir a cota afeta apenas novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

Implantar uma camada de personalização do usuário

Ao implantar o recurso de personalização do usuário, você define as políticas no Studio. Em seguida, você atribui as políticas ao grupo de entrega vinculado ao catálogo de máquinas, onde o recurso é implantado.

Se você deixar a imagem mestre sem configuração de camada de personalização do usuário, os serviços permanecerão ociosos e não interferirão nas atividades de autoria.

Se você definir as políticas na imagem mestre, os serviços tentarão executar e montar uma camada de usuário dentro da imagem mestre. A imagem mestre exibirá comportamentos inesperados e instabilidade.

Para implantar o recurso de camada de personalização do usuário, conclua as seguintes etapas nesta ordem:

- Etapa 1: Verifique a disponibilidade de um ambiente Citrix Virtual Apps and Desktops.
- Etapa 2: Prepare sua imagem mestre.
- Etapa 3: Crie um catálogo de máquinas.
- Etapa 4: Crie um grupo de entrega.
- Etapa 5: Crie políticas personalizadas de grupo de entrega.

> **Nota:**
>
> Fazer logon pela primeira vez após atualizar o Windows 10 na imagem leva mais tempo do que o normal. A camada do usuário precisa ser atualizada para a nova versão do Windows 10, o que aumenta o tempo de logon.

Etapa 1: Verifique se o ambiente Citrix Virtual Apps and Desktops está disponível

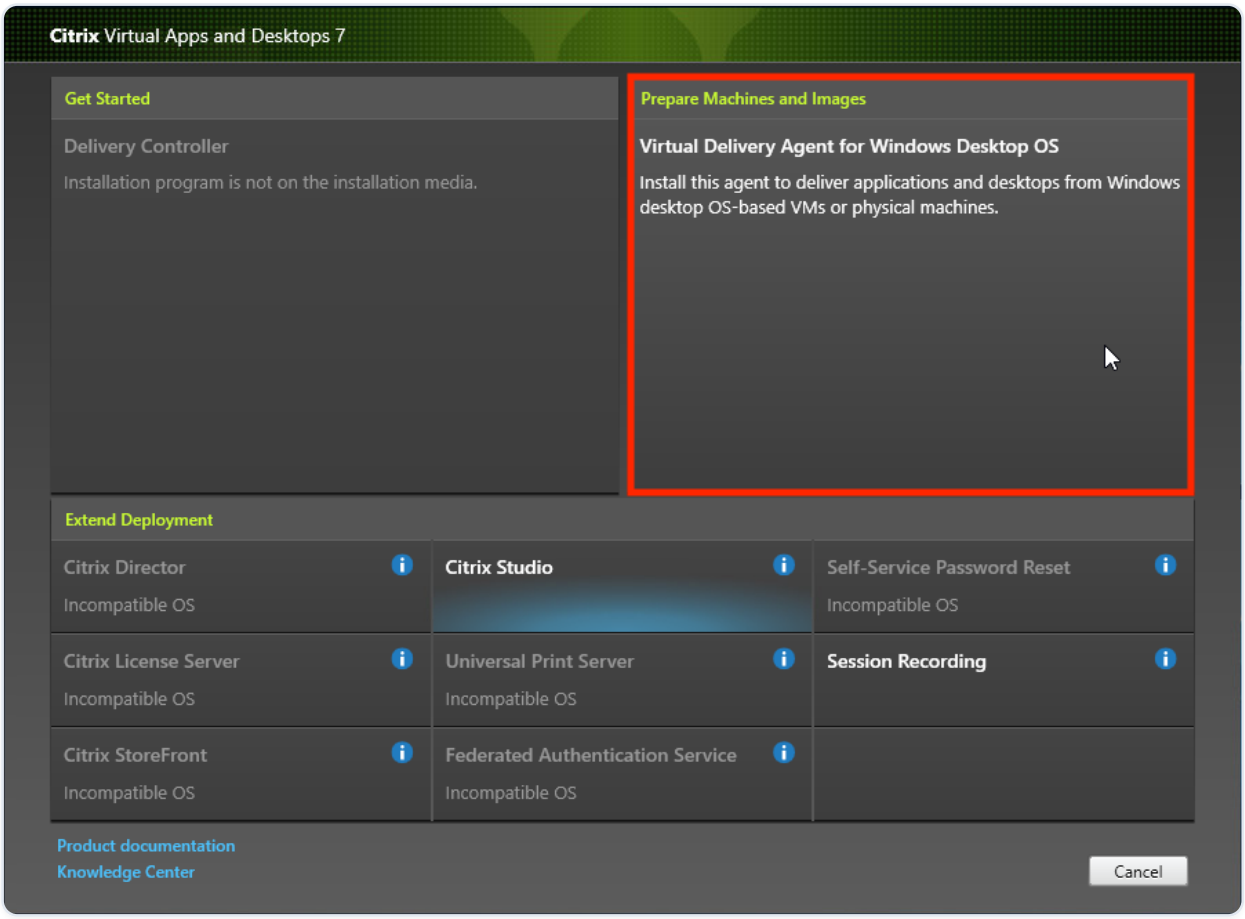
Certifique-se de que seu ambiente Citrix Virtual Apps and Desktops esteja disponível para uso com este novo recurso. Para obter detalhes de configuração, consulte Instalar e configurar o Citrix Virtual Apps and Desktops.

Etapa 2: Prepare sua imagem mestre

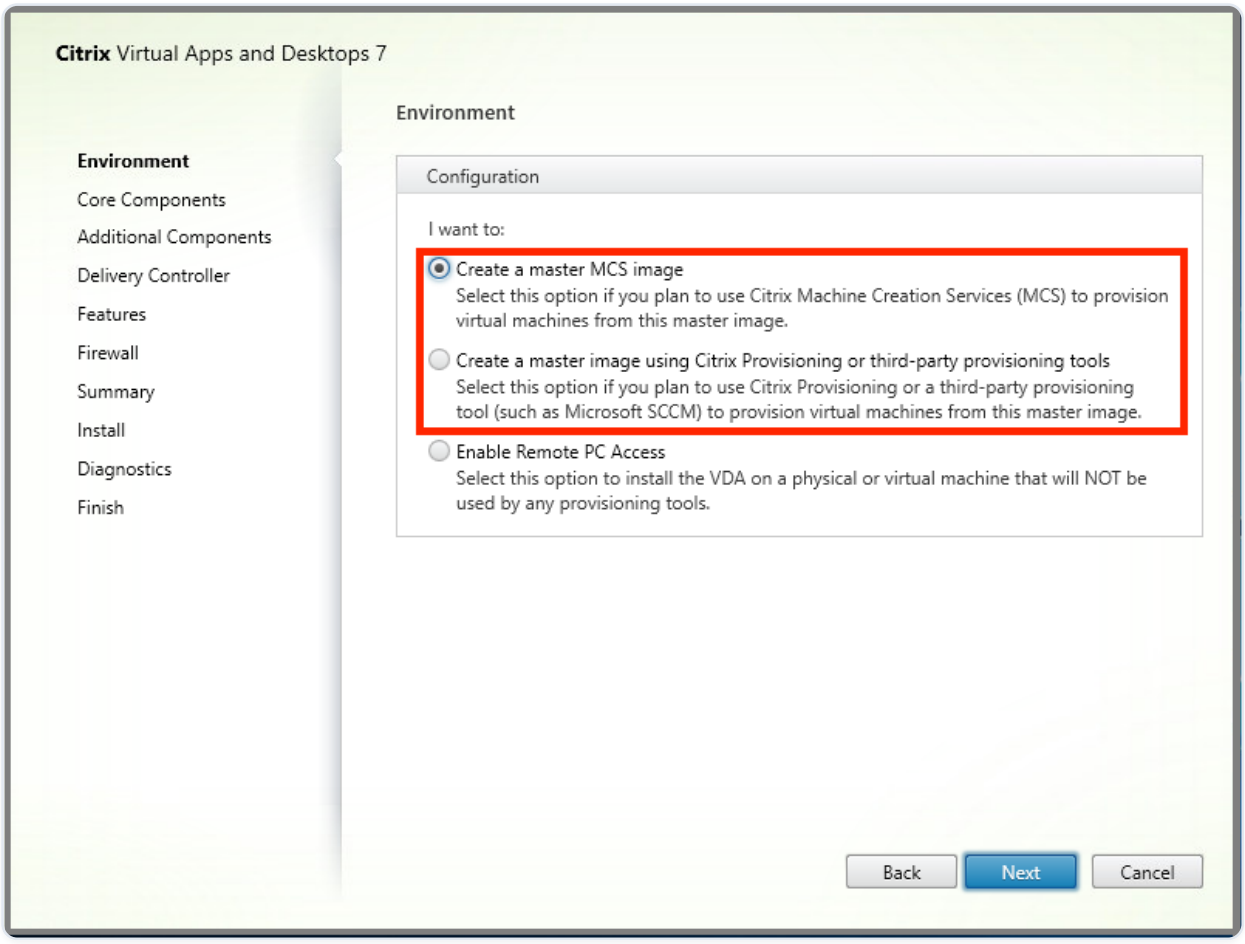
Para preparar sua imagem mestre:

1. Localize a imagem mestre. Instale os aplicativos corporativos da sua organização e quaisquer outros aplicativos que seus usuários geralmente considerem úteis.
2. Se você estiver implantando o Server VDI, siga as etapas no artigo Server VDI. Certifique-se de incluir o componente opcional, a **Camada de personalização do usuário**. Para obter detalhes, consulte as Opções de linha de comando para instalar um VDA.
3. Se você estiver usando o Windows 10, instale o Virtual Delivery Agent (VDA) 1912 ou posterior. Se uma versão mais antiga do VDA já estiver instalada, desinstale a versão antiga primeiro. Ao instalar a nova versão, certifique-se de selecionar e instalar o componente opcional, a **Camada de Personalização do Usuário Citrix**, da seguinte forma:

    a. Clique no bloco, **Virtual Delivery Agent para SO de desktop Windows**:

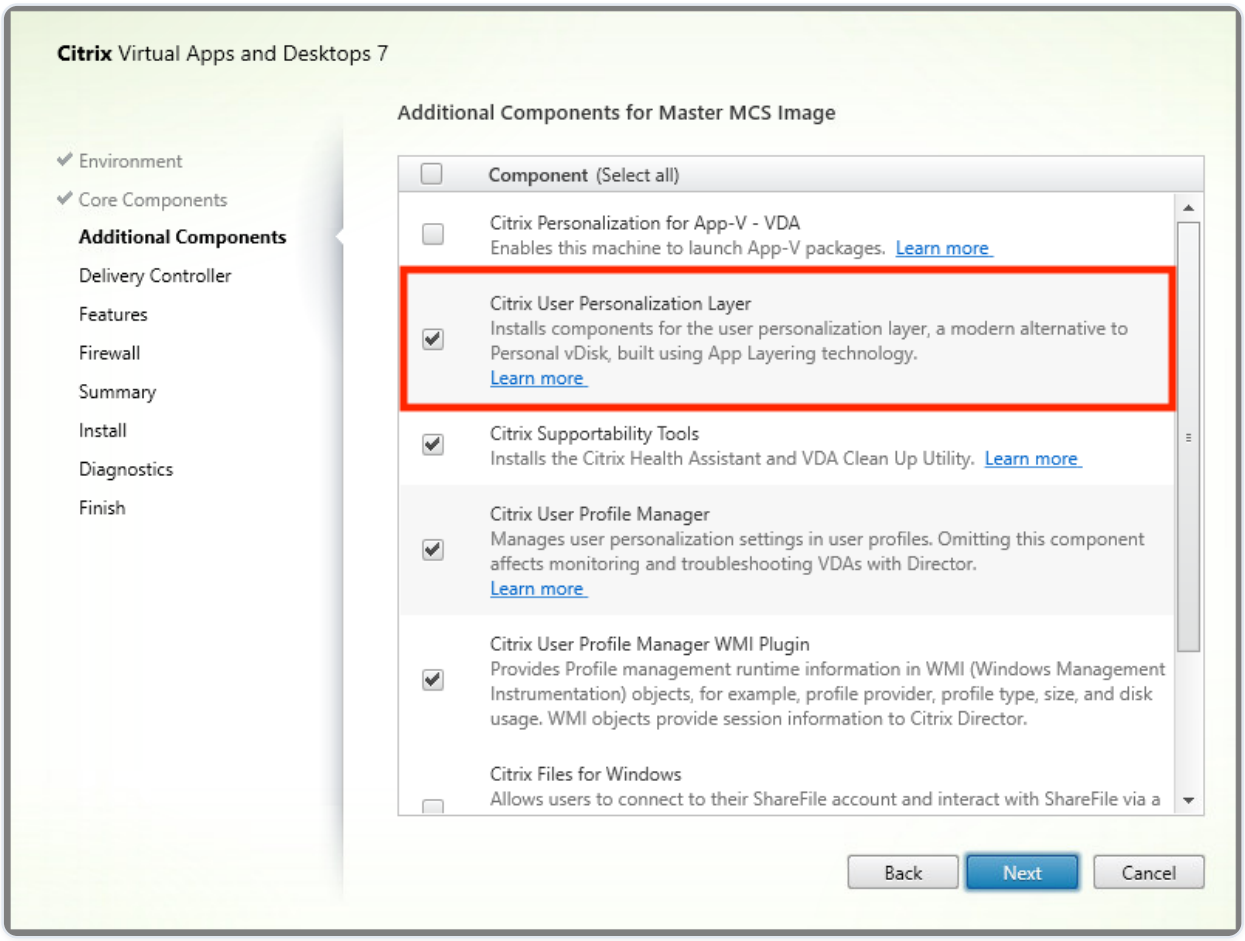


a. **Ambiente:** Selecione **Criar uma imagem mestre MCS** ou **Criar uma imagem mestre usando o Citrix Provisioning ou ferramentas de provisionamento de terceiros**.



a. **Componentes Principais:** Clique em **Avançar**.

b. **Componentes Adicionais:** Marque **Camada de Personalização do Usuário Citrix**.



a. Clique nas telas de instalação restantes, configurando o VDA conforme necessário, e clique em **Instalar**. A imagem reinicia uma ou mais vezes durante a instalação.

4. Deixe as **atualizações do Windows** desabilitadas. O instalador da camada de personalização do usuário desabilita as atualizações do Windows na imagem. Deixe as atualizações desabilitadas.

A imagem está pronta para ser carregada no Studio.

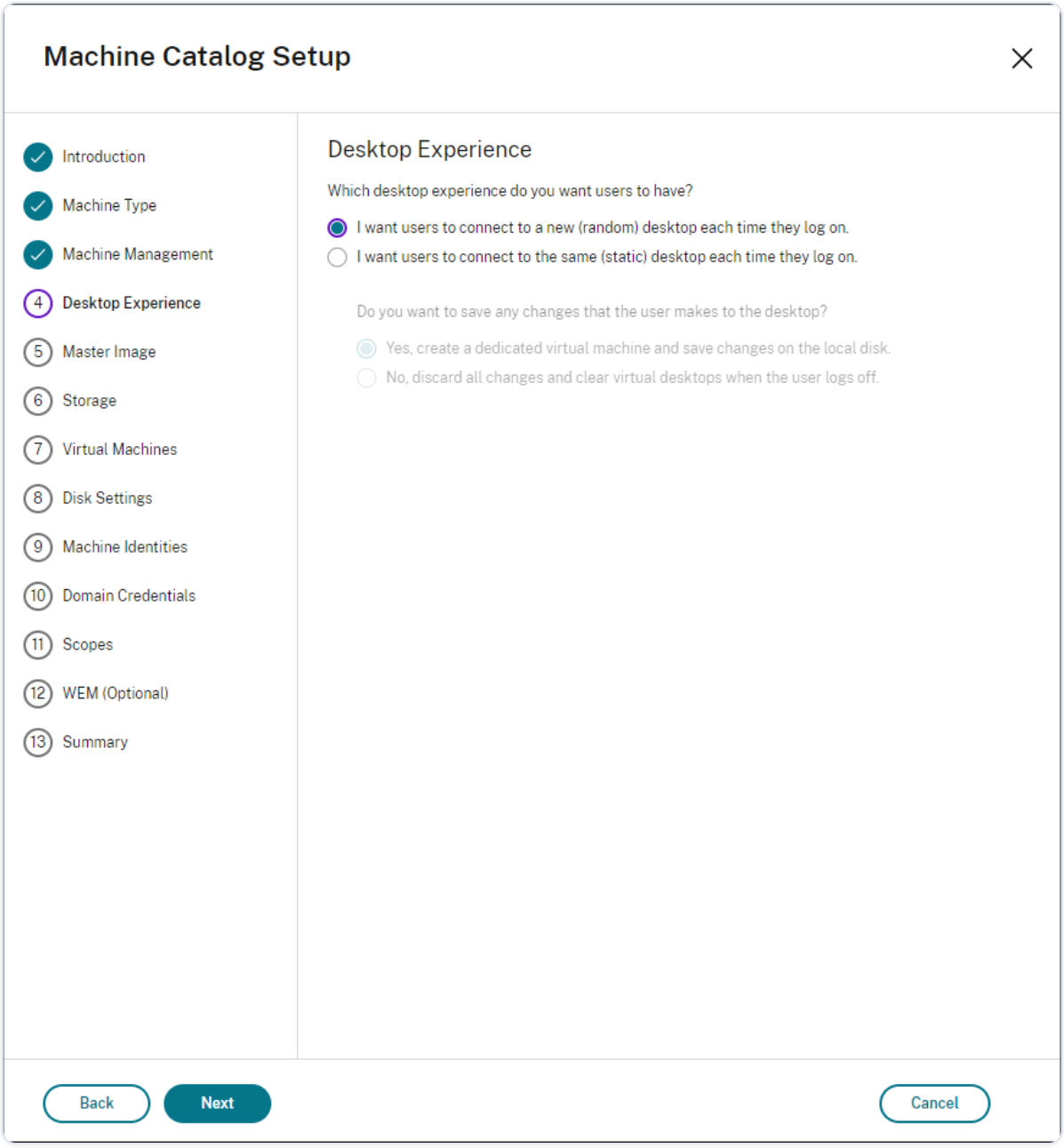
> **Nota:**
>
> Se você deseja apenas atualizar a camada de personalização do usuário (UPL), pode fazê-lo com uma versão mais recente da UPL e o pacote autônomo. Você não precisa atualizar o VDA.

Etapa 3: Criar um catálogo de máquinas

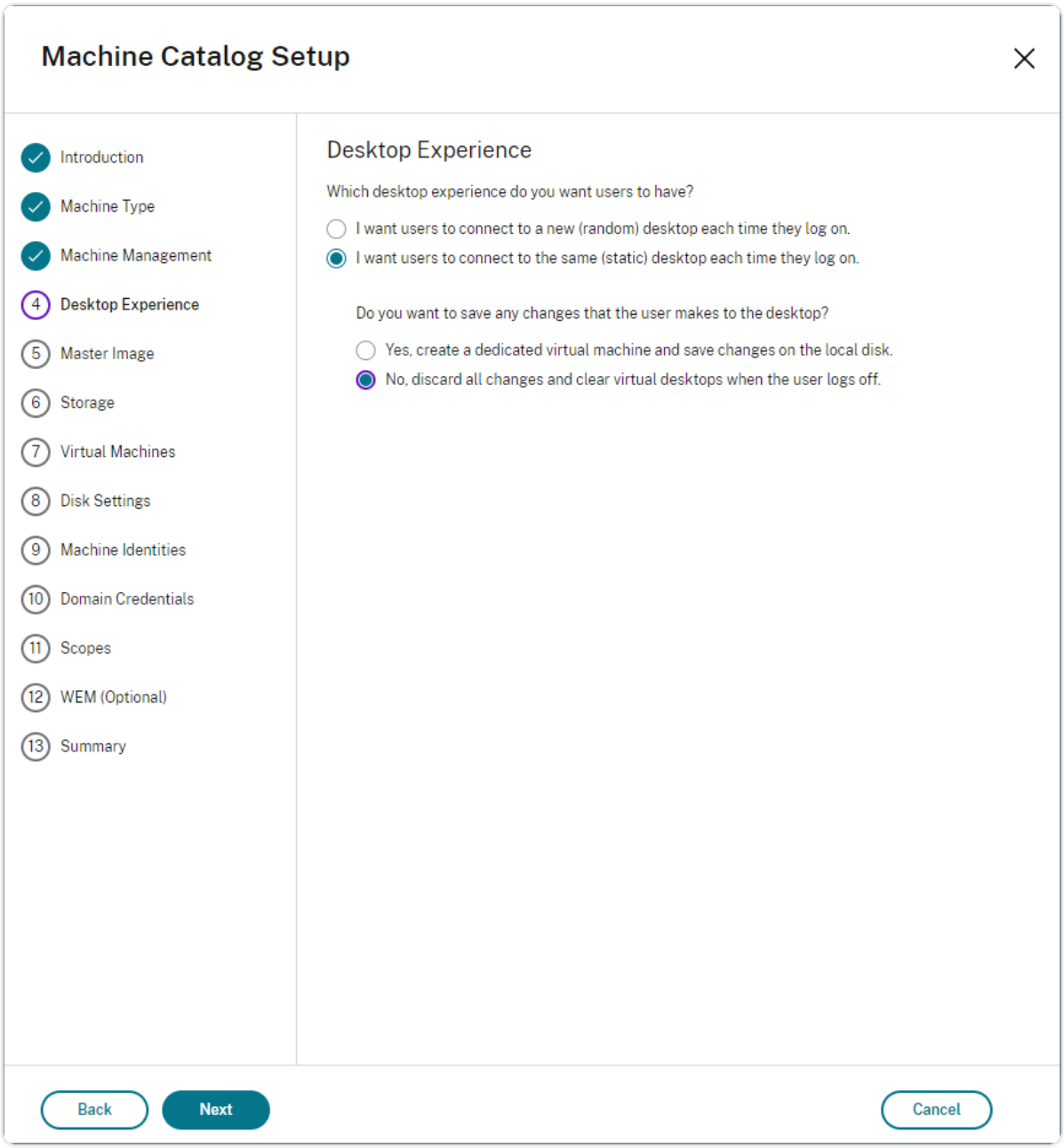
No Studio, siga as etapas para criar um catálogo de máquinas. Use as seguintes opções durante a criação do catálogo:

1. Selecione **Sistema operacional** e defina-o como **SO de sessão única**.
2. Selecione **Gerenciamento de máquinas** e defina-o como **Máquinas com gerenciamento de energia**. Por exemplo, máquinas virtuais ou PCs blade.
3. Selecione **Experiência de desktop** e defina-o como tipo de catálogo **pooled-random** ou **pooled-static**, como nos exemplos a seguir:

   - **Pooled-random:**



   - **Pooled-static:** Se você selecionar pooled-static, configure os desktops para descartar todas as alterações e limpar os desktops virtuais quando o usuário fizer logoff, conforme mostrado na seguinte captura de tela:



Nota:

A camada de personalização do usuário não oferece suporte a catálogos pooled-static configurados para usar o Citrix Personal vDisk ou atribuídos como máquinas virtuais dedicadas.

4. Se você estiver usando o MCS, selecione **Imagem** e o instantâneo da imagem criada na seção anterior.
5. Configure as propriedades restantes do catálogo conforme necessário para seu ambiente.

Etapa 4: Criar um grupo de entrega

Crie e configure um **grupo de entrega**, incluindo máquinas do catálogo de máquinas que você criou. Para obter detalhes, consulte Criar grupos de entrega.

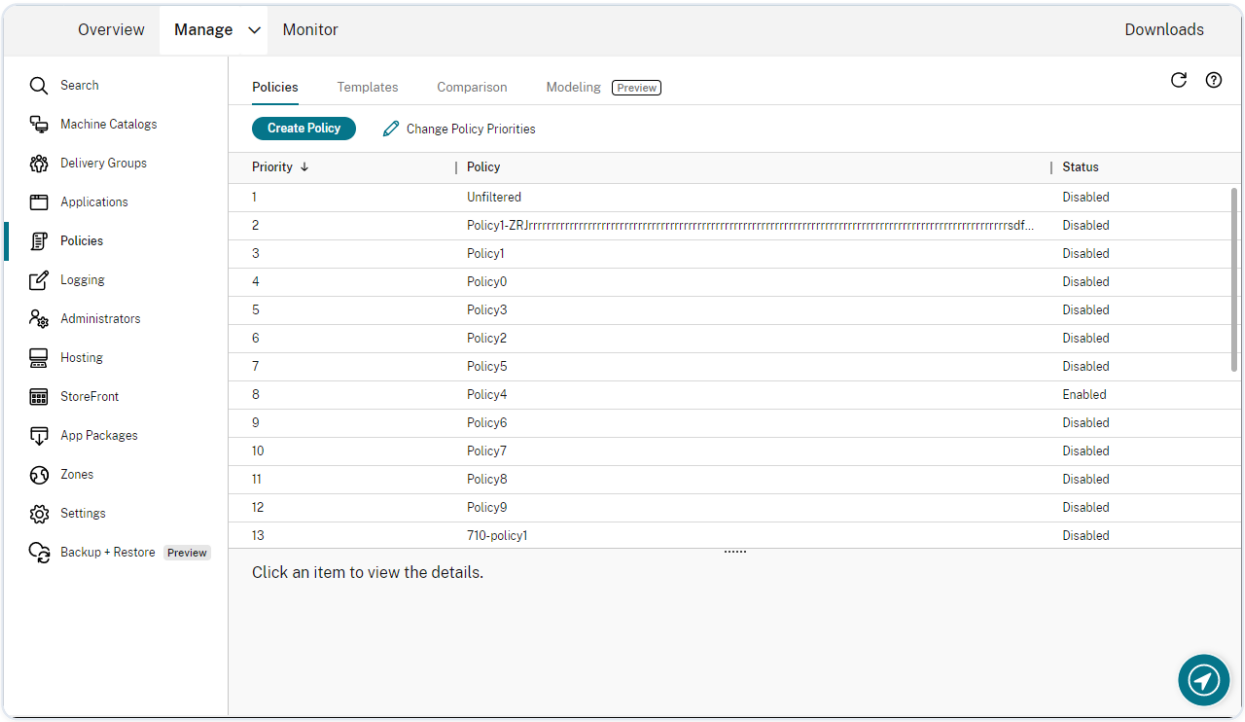
Etapa 5: Criar políticas personalizadas de grupo de entrega

Para habilitar a montagem de camadas de usuário dentro dos Virtual Delivery Agents, use os parâmetros de configuração para especificar:

- Onde na rede acessar as camadas de usuário.
- Qual o tamanho máximo permitido para o crescimento dos discos da camada de usuário.

Para definir os parâmetros como políticas personalizadas do Citrix no Studio e atribuí-los ao seu grupo de entrega.

1. Faça login no Studio e selecione **Políticas** no painel esquerdo:



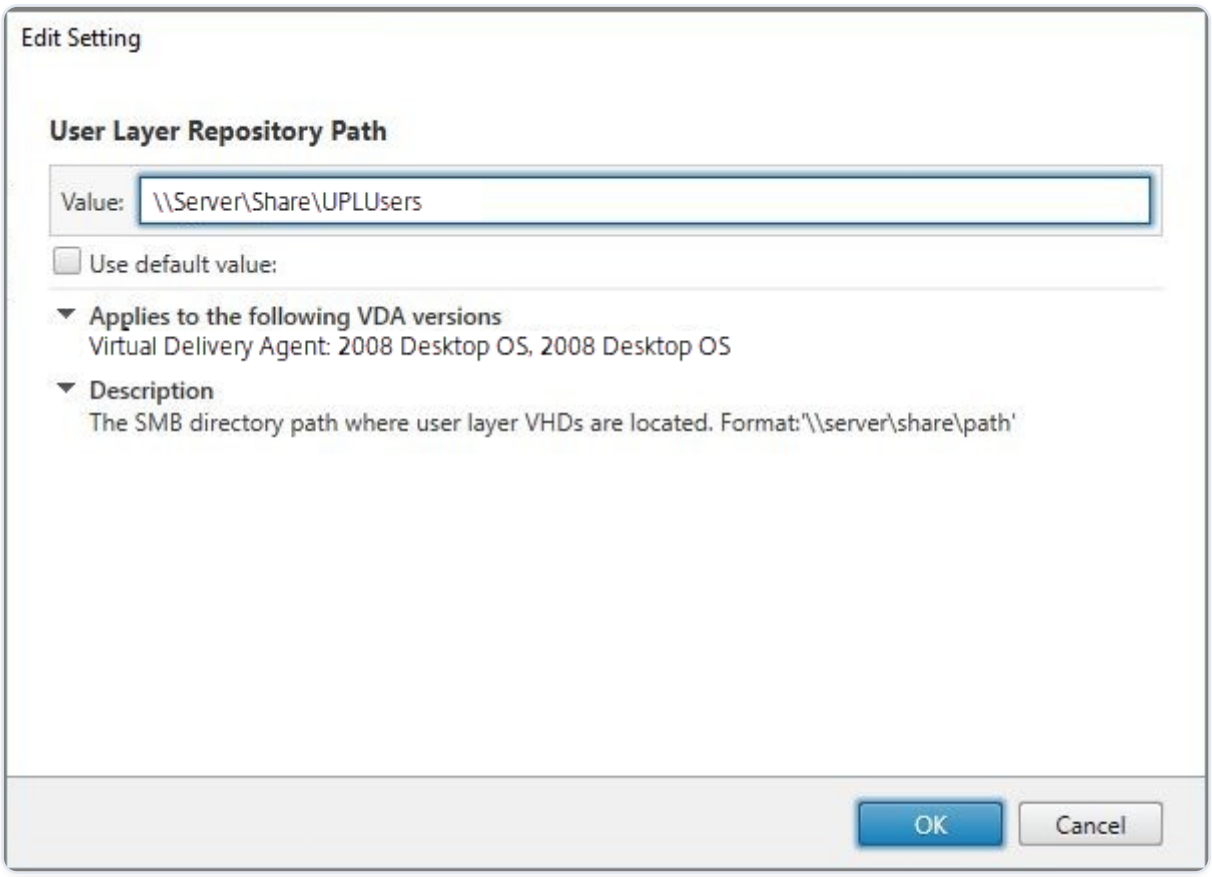
2. Selecione **Criar Política** na barra de ações. A janela Criar Política é exibida.
3. Digite 'camada de usuário' no campo de pesquisa. As três políticas a seguir aparecem na lista de políticas disponíveis:

    - Exclusões da Camada de Usuário
    - Caminho do Repositório da Camada de Usuário
    - Tamanho da Camada de Usuário em GB

> **Nota:**
>
> Aumentar o tamanho afeta novas camadas de usuário e expande as camadas de usuário existentes. Diminuir o tamanho afeta apenas novas camadas de usuário. As camadas de usuário existentes nunca diminuem de tamanho.

4. Marque a caixa de seleção ao lado de **Caminho do Repositório da Camada de Usuário** e clique em **Editar**. A janela Editar Configuração é exibida.
5. Insira um caminho no campo **Valor** e clique em **Salvar**:

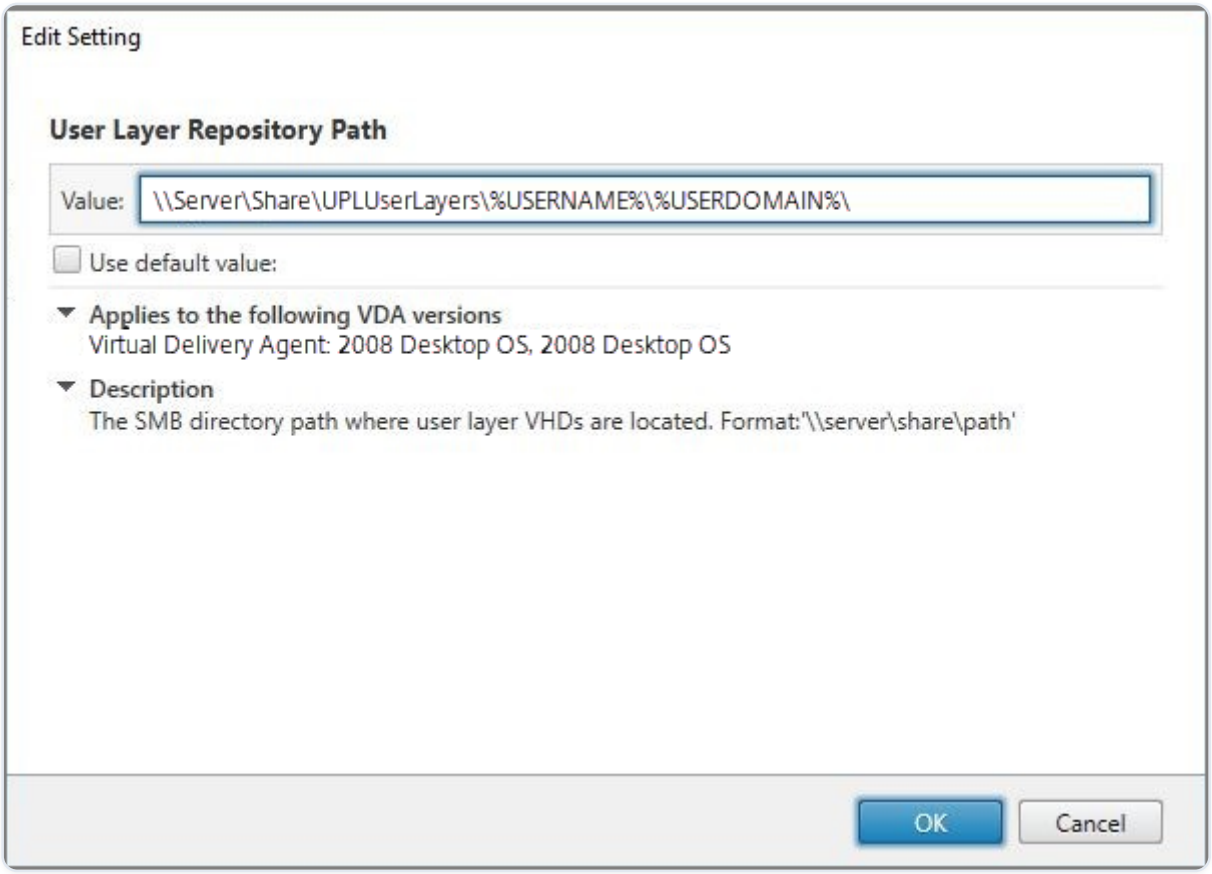
   - **Formato do caminho:** `\\server-name-or-address\share-name\folder`
   - **Exemplo de caminho:** `\\Server\Share\UPLUsers`
   - **Exemplo de caminhos resultantes:** Para um usuário chamado **Alex** em **CoolCompanyDomain**, o caminho seria: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`



Você pode personalizar o caminho usando as `%USERNAME%` e `%USERDOMAIN%` variáveis, variáveis de ambiente da máquina e atributos do Active Directory (AD). Quando expandidas, essas variáveis resultam em caminhos explícitos.

Exemplo de variáveis de ambiente:

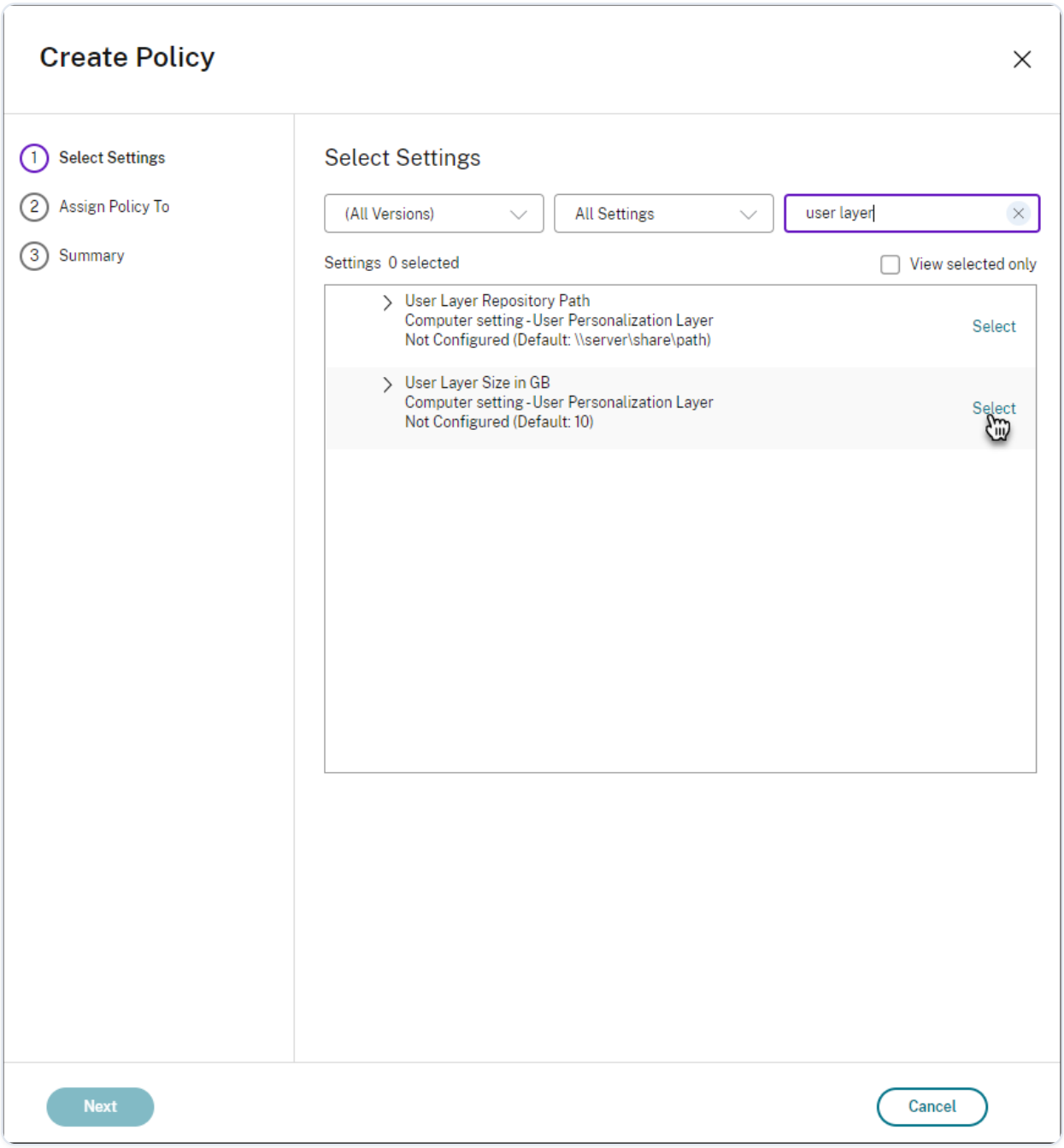
- **Formato do caminho:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Exemplo de caminho:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **Exemplo de caminhos resultantes:** Para um usuário chamado **Alex** em **CoolCompanyDomain**, o caminho seria: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`



Exemplo de atributos AD personalizados:

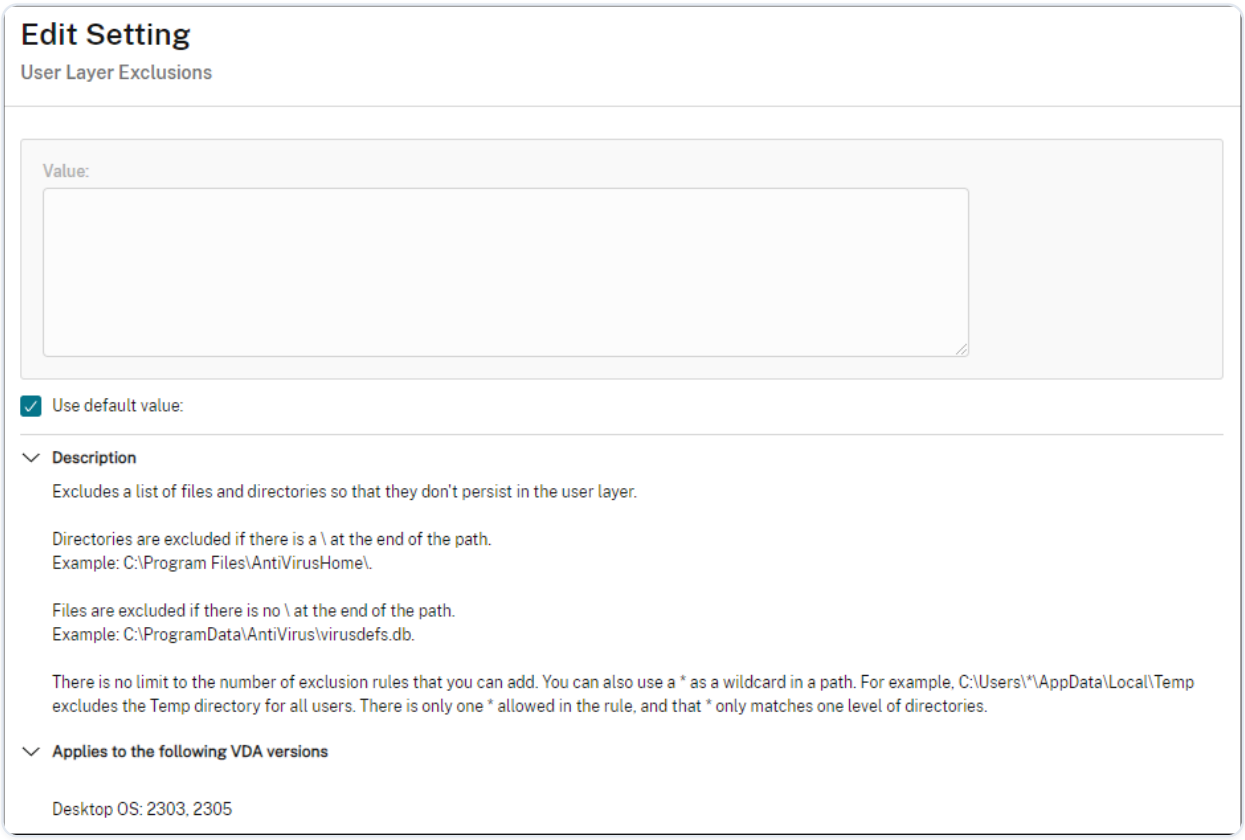
- Formato do caminho: `\\Server-name-or-address\share-name\AD-attribute`
- Exemplo de caminho: `\\Server\share#sAMAccountName#`
- Exemplo de caminhos resultantes: `\\Server\share\JohnSmith` (se #sAMAccountName# resolver para JohnSmith para o usuário atual)

6. Opcional: Marque a caixa de seleção ao lado de **Tamanho da Camada de Usuário em GB** e clique em **Editar**:

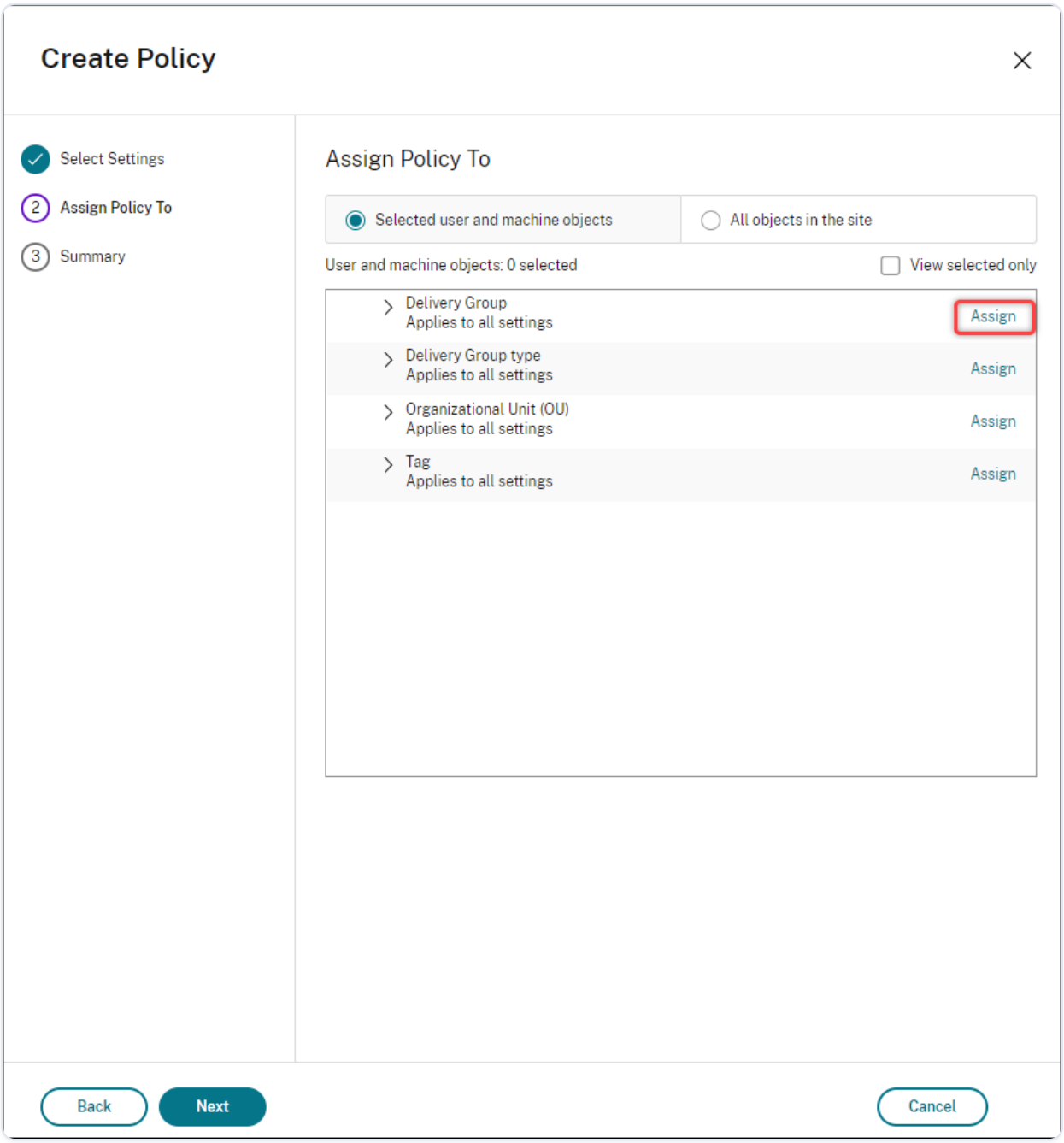


A janela Editar Configurações é exibida.

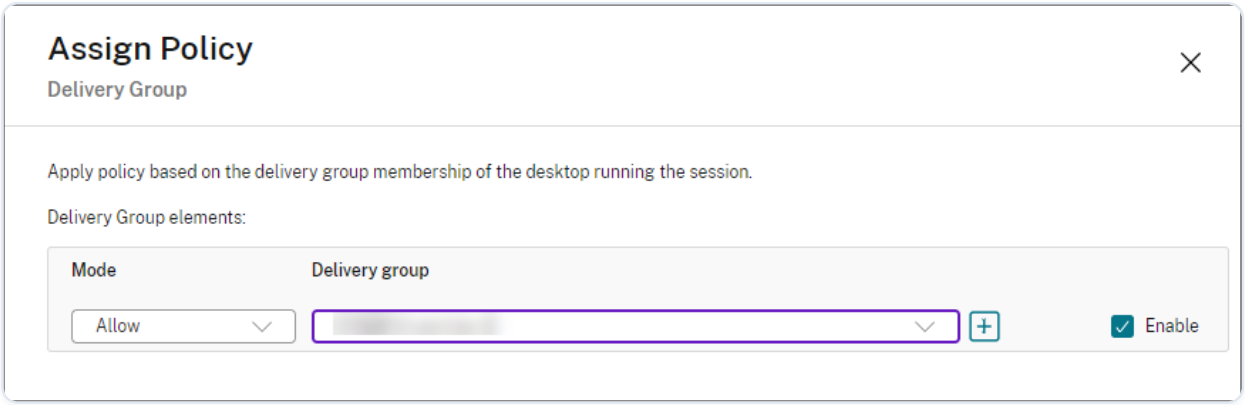
7. Opcional: Altere o valor padrão de **10 GB** para o tamanho máximo que cada camada de usuário pode atingir. Clique em **Salvar**.
8. Opcional: Marque a caixa de seleção ao lado de **Exclusões da Camada de Usuário** e clique em **Editar**.



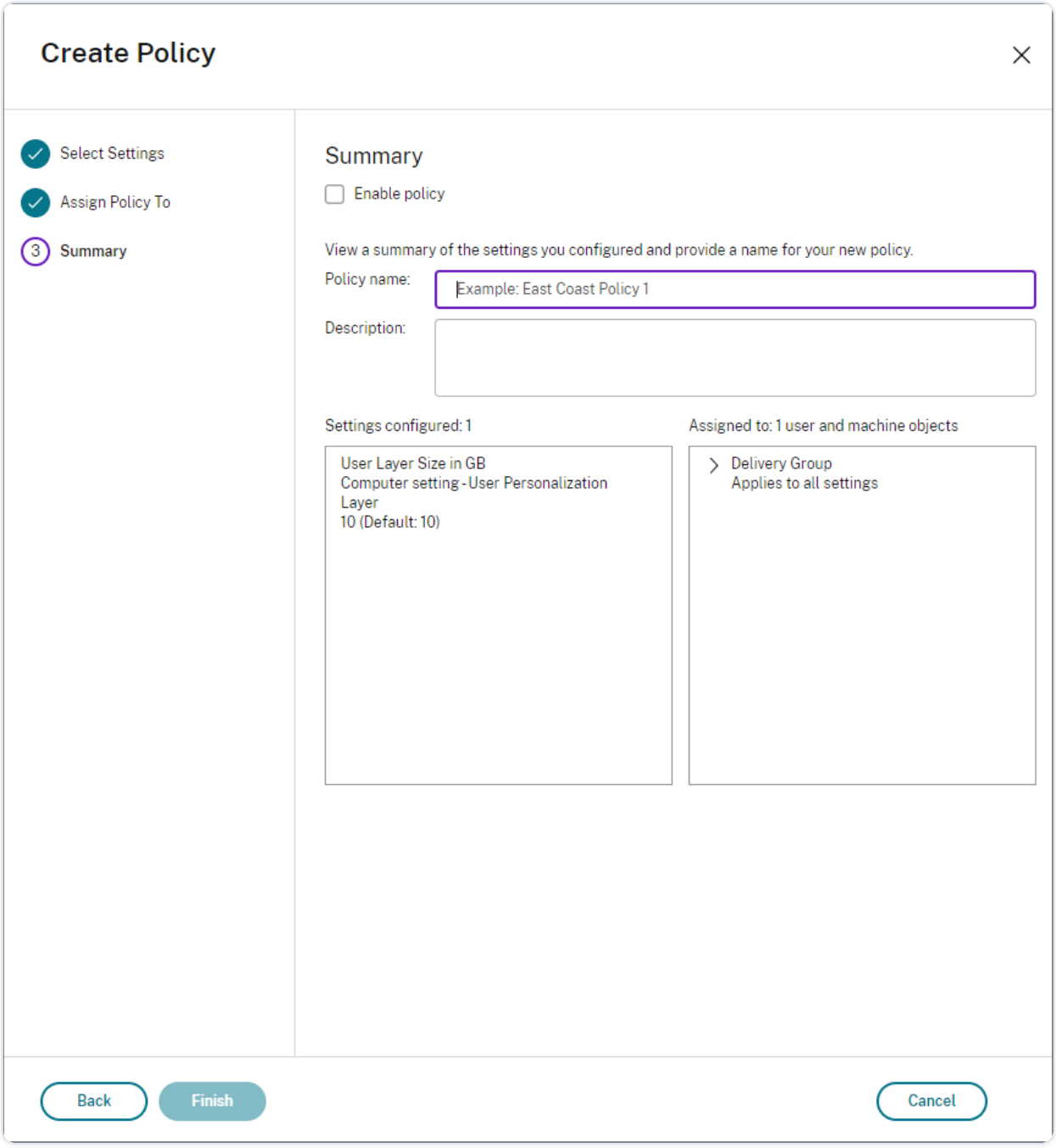
9. Opcional: Especifique os arquivos e pastas a serem excluídos e clique em **Salvar**. Para obter mais informações, consulte a documentação do Citrix App Layering.
10. Clique em **Avançar** para configurar os usuários e máquinas aos quais você deseja atribuir. Clique no link **Atribuir Grupo de Entrega** destacado nesta imagem:



11. No menu **Grupo de Entrega**, selecione o grupo de entrega criado na seção anterior. Clique em **OK**.



12. Insira um nome para a política. Marque a caixa de seleção para habilitar a política e clique em **Concluir**.



Configurar as configurações de segurança na pasta da camada de usuário

Como administrador de domínio, você pode especificar mais de um local de armazenamento para suas camadas de usuário. Crie uma subpasta `\Users` para cada local de armazenamento (incluindo o local padrão). Proteja cada local usando as seguintes configurações.

NOME DA CONFIGURAÇÃO	VALOR	APLICAR A	
Criador/Proprietário	Modificar	Somente subpastas e arquivos	
Direitos do Proprietário	Modificar	Somente subpastas e arquivos	
Usuários ou grupo	Criar Pasta/Anexar Dados; Atravessar Pasta/Executar Arquivo; Listar Pasta/Ler Dados; Ler Atributos	Somente Pasta Selecionada	
Sistema	Controle Total	Pasta Selecionada, Subpastas e Arquivos	
Administradores de Domínio e grupo de Administradores selecionado	Controle Total	Pasta Selecionada, Subpastas e Arquivos	

Mensagens da camada de usuário

Quando um usuário não consegue acessar sua camada de usuário, ele recebe uma destas mensagens de notificação.

- **Camada de Usuário em Uso**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **Camada de Usuário Indisponível**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **Sistema não redefinido após o logout do usuário**

`This system was not shut down properly. Please log off immediately and contact your system administrator.`.

Arquivos de log para usar na solução de problemas

O arquivo de log, ulayersvc.log, contém a saída do software da camada de personalização do usuário onde as alterações são registradas.

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

Limitações

Tenha as seguintes limitações em mente ao instalar e usar o recurso de camada de personalização do usuário.

- NÃO *tente* implantar o software da camada de personalização do usuário em uma camada dentro do App Layering. Implante as camadas de personalização do usuário no Citrix Virtual Apps and Desktops, OU habilite as camadas de usuário em um modelo de imagem do App Layering, mas não ambos. Qualquer um dos processos produz as camadas de usuário de que você precisa.
- Não *configure* o recurso de camada de personalização do usuário com catálogos de máquinas persistentes.
- Não *use* hosts de sessão.
- Não *atualize* o catálogo de máquinas com uma imagem executando uma nova instalação do SO (mesmo que seja a mesma versão do Windows 10). A melhor prática é aplicar as atualizações ao SO dentro da mesma imagem mestre usada ao criar o catálogo de máquinas.
- Não *use* drivers de tempo de inicialização, nem qualquer outra personalização de inicialização antecipada.
- Não *migre* dados de PvD para o recurso de camada de personalização do usuário.
- Não *migre* camadas de usuário existentes do produto App Layering completo para o recurso de camada de personalização do usuário.
- Não *altere* o caminho SMB da camada de usuário para acessar camadas de usuário criadas usando uma imagem de SO mestre diferente.
- Quando um usuário faz logoff de uma sessão e depois faz login novamente, a nova sessão é executada em uma máquina diferente no pool. Em um ambiente VDI, o Microsoft Software

Center lista um aplicativo como **Instalado** na primeira máquina, mas o mostra como **Indisponível** na segunda máquina.

Para descobrir o status real do aplicativo, instrua o usuário a selecionar o aplicativo no Software Center e clicar em **Instalar**. O SCCM então atualiza o status para o valor real.

- O Software Center ocasionalmente para imediatamente após ser iniciado em um VDA que tem o recurso de camada de personalização do usuário habilitado. Para evitar esse problema, siga as recomendações da Microsoft para Implementar o SCCM em um ambiente VDI XenDesktop. Além disso, certifique-se de que o serviço `ccmexec` esteja em execução antes de iniciar o Software Center.
- Nas Políticas de Grupo (Configurações do Computador), as configurações da camada de usuário substituem as configurações aplicadas à imagem mestre. Portanto, as alterações feitas nas Configurações do Computador usando uma GPO nem sempre estão presentes para o usuário no próximo login da sessão.

  Para contornar esse problema, crie um Script de Logon do Usuário que emita o comando:

  ```
  gpupdate /force
  ```

  Por exemplo, um cliente configurou o seguinte comando para ser executado em cada login de usuário:

  ```
  gpudate /Target:Computer /force
  ```

  Para melhores resultados, aplique as alterações nas Configurações do Computador diretamente na camada do usuário, depois que o usuário tiver feito login.
- Uma conta de usuário de domínio não deve ser o último usuário a ter feito login em uma imagem mestre. Caso contrário, as máquinas provisionadas a partir dessa imagem terão problemas.
- Certificados personalizados não persistem quando o UPL está habilitado em um ambiente Microsoft Entra puro, devido a um problema subjacente no Windows em execução no Azure. Se a Microsoft corrigir esse problema em um aprimoramento futuro, atualizaremos este artigo.

Fazer backup ou migrar sua configuração

Este recurso ajuda você a fazer backup de suas configurações DaaS. O backup, juntamente com o recurso de restauração, facilita a migração de informações do site do local para a nuvem ou de um site em nuvem para outro com facilidade. Ele também facilita a recuperação imediata de um site em momentos de emergência.

Você pode usar os seguintes métodos para fazer backups:

1. Backup + Restauração
    a. Integrado com o Studio.
2. Ferramenta de Configuração Automatizada (ACT)
    a. Ferramenta baseada em PowerShell. Instale a ferramenta para usá-la. Consulte Baixar Configuração Automatizada.

Os backups podem ser usados para:

1. Restauração
2. Migração

A Citrix® recomenda as seguintes ferramentas para os cenários descritos.

Backup

AMBIENTE	CASO DE USO	FERRAMENTA RECOMENDADA	CONSIDERAÇÕES ESPECIAIS	LINK
DaaS e no local	Backups sob demanda e agendados	Backup + Restauração	A Citrix mantém o backup e o usuário pode baixá-lo se necessário	Backup e Restauração usando o Studio

AMBIENTE	CASO DE USO	FERRAMENTA RECOMENDADA	CONSIDERAÇÕES ESPECIAIS	LINK
DaaS e no local	Backups sob demanda e agendados	ACT	O usuário mantém o backup	Backup e Restauração usando a Ferramenta de Configuração Automatizada

Migração

AMBIENTE	CASO DE USO	FERRAMENTA RECOMENDADA	CONSIDERAÇÕES ESPECIAIS	LINK
No local para a nuvem	Migrar um site local para DaaS	ACT		Migrar do local para a nuvem
	Consolidar vários sites locais em um site DaaS	ACT	Fusão de sites	Mesclar vários sites locais em um único site na nuvem
No local para no local	Migrar um site local para outro site local	ACT		Guia de POC:Ferramenta de Configuração Automatizada - Migração local para local
	Consolidar vários sites locais em outro site local	ACT	Fusão de sites	Guia de POC:Ferramenta de Configuração Automatizada Migração local para local

AMBIENTE	CASO DE USO	FERRAMENTA RECOMENDADA	CONSIDERAÇÕES ESPECIAIS	LINK
				Mesclar vários sites locais em um único site na nuvem
Nuvem para nuvem	Migrar um site DaaS para outro site DaaS	ACT		Migrar da nuvem para a nuvem
Consolidar vários sites DaaS em um único site DaaS	Fusão de sites	ACT		Migrar da nuvem para a nuvem(/pt-br/citrix-daas/backup-migrate-configuration/migrate-cloud-to-cloud.html#prerequisites-for-migrating-your-configuration)
				Migrar vários sites locais para um único site na nuvem(/pt-br/citrix-daas/backup-migrate-configuration/multi-site-merge.html)

Configuração de Backup e Restauração

Este recurso permite que os administradores façam backup de suas configurações de nuvem. Ele garante que sempre haja uma cópia de suas configurações Citrix® disponível, pronta para ser

usada. O backup, juntamente com o recurso de restauração, facilita a migração de informações do site de ambientes locais para a nuvem ou de um site de nuvem para outro com facilidade. Se ocorrerem alterações acidentais, escolha um backup e selecione restaurar, e com alguns cliques, você estará novamente em funcionamento. Você também pode optar por fazer backup e restaurar componentes específicos.

O recurso permite fazer backup e restaurar o seguinte:

- Tags
- AdminRoles
- AdminScopes
- HostConnections

> **Nota:**
>
> Agora você pode fazer backup de Host Connections no DaaS. Os segredos devem ser inseridos a cada vez. Um modo de verificação de pré-importação é executado para solicitar segredos apenas para as Host Connections que são importadas ou atualizadas.

- StoreFront™
- Grupos de entrega
- ApplicationGroups
- Aplicativos
- AppVIsolationGroups
- AppLibPackageDiscovery
- Políticas de Grupo
- Preferência de Zona do Usuário
- Catálogos de máquinas provisionados manualmente ou provisionados por PVS
- Pastas de administrador
  - Pastas de aplicativos
  - Pastas de grupos de entrega
  - Pastas de catálogos de máquinas
- Configurações do Site

> **Importante:**
>
> Certifique-se de seguir a ordem da lista fornecida acima para restaurar diferentes componentes. Por exemplo, se você deseja restaurar Aplicativos, Grupos de entrega e Políticas de grupo, você deve seguir a ordem:
>
> - Grupos de entrega
> - Aplicativos
> - Políticas de grupo.

> **Nota:**
>
> Não é possível fazer backup ou restaurar catálogos de máquinas MCS.

Tipo de backups

Use as seguintes opções para realizar backups de acordo com seus requisitos:

- **Sob demanda**: Faz backup das configurações do site em tempo real. Esta ação faz backup das configurações atuais do site Citrix Cloud™.
- **Agendado**: Faz backup das configurações do site em intervalos agendados. Isso se repete nos intervalos mencionados.

> **Nota:**
>
> Somente administradores com direitos totais e administradores de nuvem podem fazer backups e restaurações sob demanda ou agendados.

Backup e Restauração usando o Studio

Este artigo descreve as ações que você pode realizar no nó **Backup e Restauração** disponível no painel esquerdo do seu console Gerenciar DaaS.

Backup e Restauração permite ao administrador fazer backups do Studio.

Criar backups sob demanda

1. Faça login no Citrix Cloud.
2. Clique no bloco **DaaS**.
3. No menu esquerdo, selecione **Backup e Restauração**.
4. Na guia **Backup e Restauração**, clique em **Criar backup**.
5. Na página **Criar backup**, insira as notas e clique em **Criar backup**.

   Uma atividade de resumo é exibida mostrando os componentes de backup sendo copiados em nome do administrador que aciona o backup.
6. Após o backup ser concluído com sucesso, ele é listado como um item na guia **Backup e Restauração**.
7. Selecione um backup específico para ver mais informações sobre o backup na guia **Detalhes**.

Para excluir um backup, clique com o botão direito do mouse em um backup e clique em **Excluir backup**.

Fixar um backup

A Citrix® armazena os últimos 30 backups. Quando você cria mais de 30 backups, o sistema exclui os backups antigos na ordem em que foram criados. Para cada novo backup criado além do limite de 30 backups, o sistema exclui o backup que foi criado primeiro. A fixação de backup é usada para evitar a exclusão automática de um backup específico. Você pode fixar até 5 backups. Caso haja backups fixados, retemos todos os backups fixados além dos 30 backups, ou seja, no máximo, você pode reter 35 backups – 30 não fixados e 5 fixados.

1. Clique com o botão direito em um backup para fixar.

Criar backups agendados

Crie um agendamento de backup que se alinhe aos requisitos da sua organização para automatizar seus processos de backup e restauração. Os backups operam em segundo plano em uma frequência que você selecionar (diária, semanal, mensal ou outra frequência adequada).

1. Vá para a guia de agendamento e selecione **Criar Agendamento**.
2. Na página **Criar agendamento**, insira o seguinte:

   - **Habilitar este agendamento**. Escolha **sim** para habilitar este agendamento de backup.
   - **Nome**. Insira um nome para o agendamento de backup.
   - **Descrição**. Insira uma descrição.

- **Fuso horário**. Selecione o fuso horário de sua escolha.
- **Frequência**. Selecione a frequência para executar o backup.
- **Repetir a cada**. Insira o número de dias após os quais o agendamento deve ser repetido.
- **Data de início**. Insira a data de início.
- **Iniciar backup em**. Insira a hora em que você deseja que o backup comece, no formato de 24 horas.

3. Selecione **Concluído**.

Limitar backups agendados

Você pode limitar os backups agendados a um por dia para evitar backups idênticos.

1. Vá para a guia **Configurações** do nó **Backup e Restauração**.
2. Clique em **Alterar** na caixa **Backups agendados**.
3. Alterne o botão para habilitar o limite de backups agendados para um por dia.

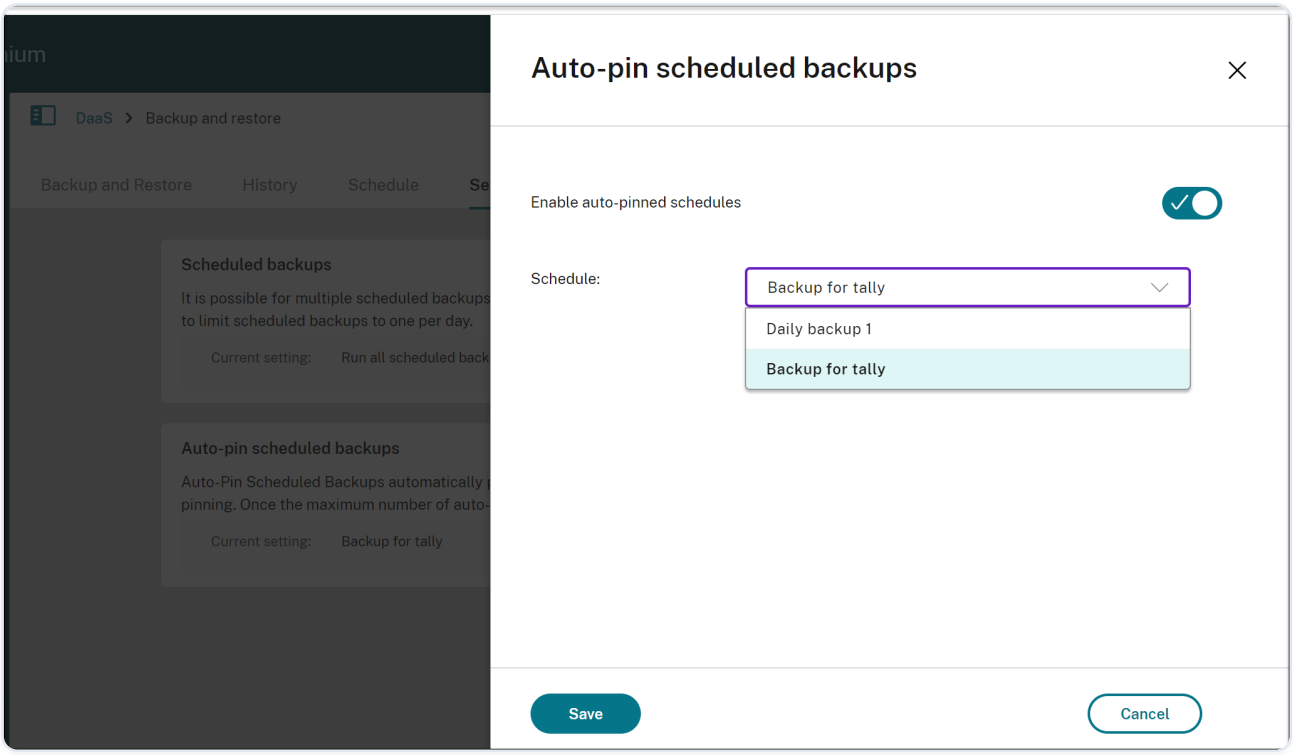
Fixar automaticamente backups agendados

A fixação automática de backups agendados fixa automaticamente os backups criados pelo agendamento selecionado. Apenas um agendamento pode ser selecionado para fixação automática.

Usando a fixação automática de backups agendados, você pode reter um máximo de seis backups agendados. Quando o limite máximo é atingido, o backup fixado automaticamente mais antigo é excluído.

> **Nota:**
>
> A Citrix armazena até seis backups fixados automaticamente. O sistema exclui backups antigos na ordem em que foram criados após o sexto backup. Para cada novo backup criado além do limite de seis backups, o sistema exclui o backup que foi criado primeiro.

1. Vá para a guia **Configurações** do nó **Backup e Restauração**.
2. Selecione um backup agendado para fixação automática.
3. Alterne o botão para habilitar agendamentos fixados automaticamente.
4. Selecione um agendamento e clique em **Salvar**.



Restaurar

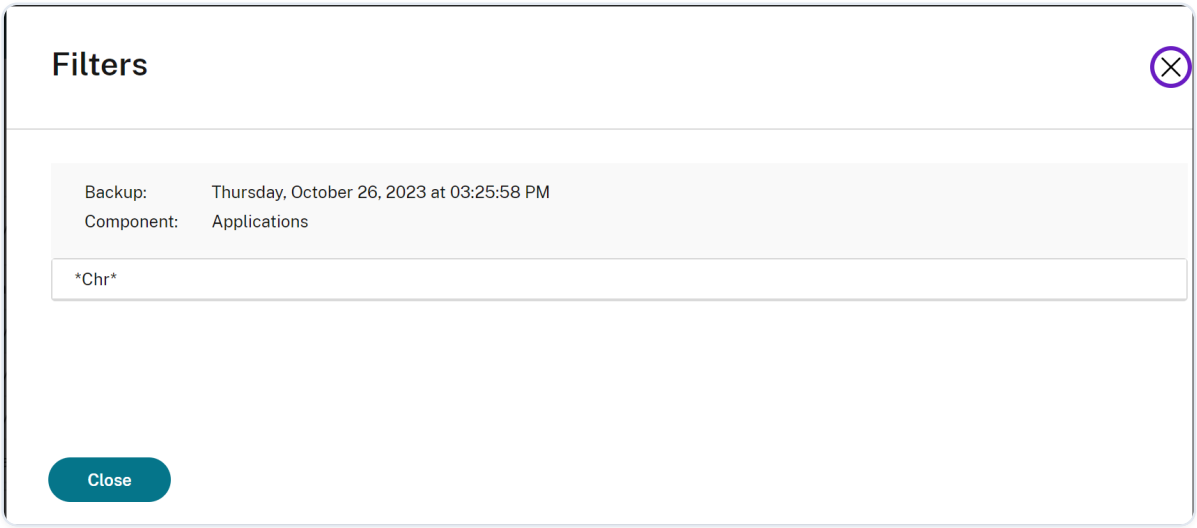
Este recurso permite que os administradores restaurem as configurações do site a partir dos backups. Permitimos que você restaure um componente por vez.

Nota:

- Restaurar apenas um componente por vez garante que não haja conflitos durante a restauração devido às dependências entre os componentes.
- O fluxo de trabalho para restaurar conexões de host é diferente de outros componentes, pois você precisaria inserir o segredo toda vez que tentar restaurar a conexão de host. Depois de clicar em **Restaurar Backup**, você deverá ver uma caixa de diálogo para inserir o segredo. Por exemplo, para o Azure, insira o segredo do aplicativo alfanumérico usado para criar a conexão.

1. Clique com o botão direito do mouse em um backup específico da lista e clique em **Restaurar Backup**.
2. Na janela **Restaurar Backup**, insira o seguinte:
   - **Componentes**: Selecione os componentes que você deseja restaurar.

- **Filtros**: Especifique os nomes dos membros que você deseja restaurar em uma lista separada por vírgulas. Por exemplo, filtrar pela palavra *chrome* restaura apenas objetos com o nome chrome. Da mesma forma, a frase `chr` restaura objetos que começam com `chr`.



Para visualizar os membros do componente, selecione um backup e navegar para **Detalhes > Componentes**. Selecione um componente e clique em **Visualizar membros do componente**.

- **Modo de verificação**: Escolha **sim** para confirmar o que deve ser restaurado quando uma operação de restauração real for concluída. Esta opção pré-avalia tudo o que é necessário para uma restauração sem realmente acioná-la. Por exemplo, ela exibe a lista de aplicativos que serão restaurados quando o processo de restauração for executado para o componente de aplicativos.

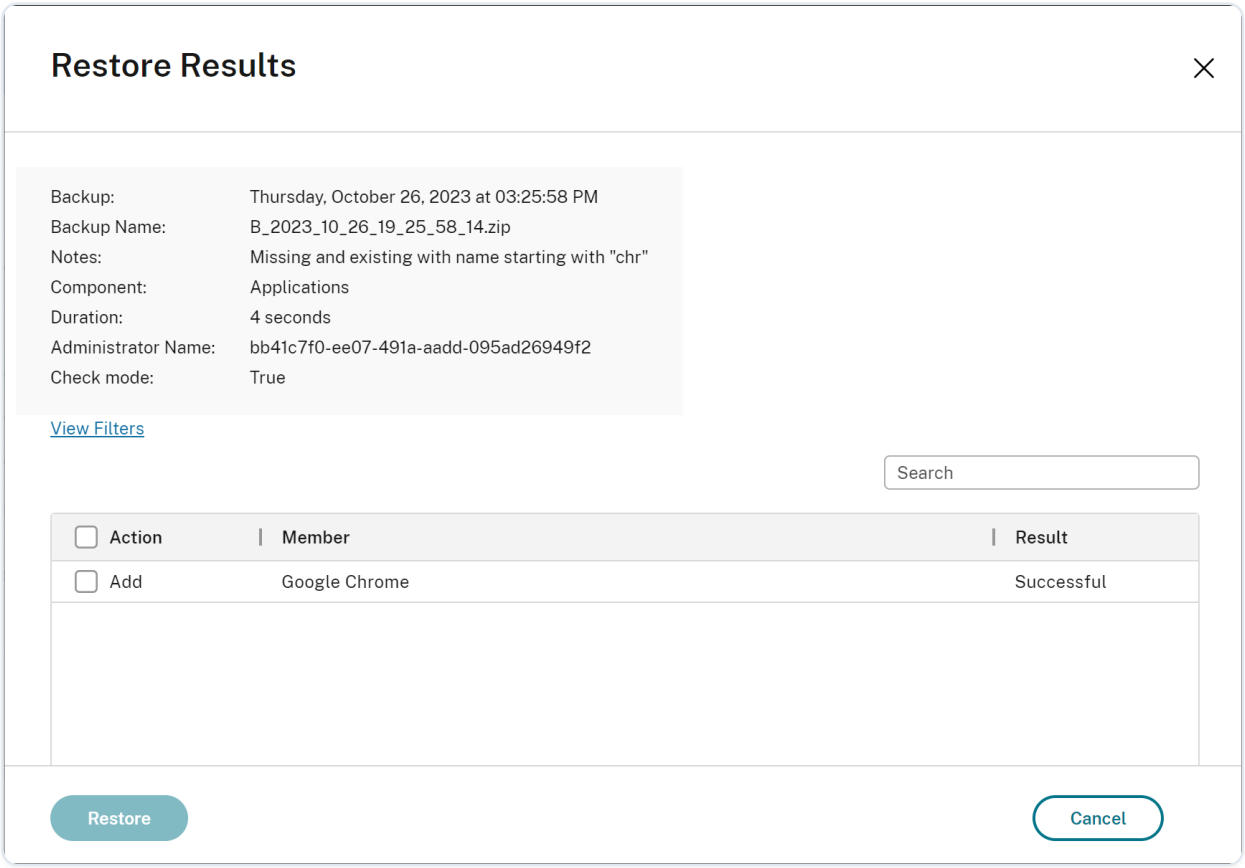
> **Nota:**
>
> O modo de verificação não executa a restauração real. Esta opção também não verifica quaisquer dependências entre os componentes. Para obter resultados ótimos, recomendamos usar o modo de verificação em um componente por vez.

- **Tipo de restauração**: Escolha uma das opções:
  - **Somente ausentes**: Use este tipo de restauração para adicionar componentes e membros a um site. Esta opção não altera os componentes e membros existentes, mesmo que o backup que está sendo restaurado tenha configurações diferentes.
  - **Ausentes e atualizando existentes**: Use este tipo de restauração para adicionar e atualizar componentes a um site. Esta opção atualiza os componentes e membros

existentes com as configurações do backup se ambos tiverem configurações diferentes.

- **Notas**: Insira quaisquer notas.

3. Selecione **Restaurar**.



Os resultados da restauração são listados na janela **Restaurar** após a conclusão da ação de restauração. Todas as ações de restauração são listadas na guia **Histórico**.

Histórico

Você pode rastrear todas as ações de backup e restauração na guia **Histórico**.

Em **Ações**, você pode ver todos os backups excluídos e o histórico de backup.

Para visualizar detalhes sobre um backup:

1. Vá para a guia **Histórico**.
2. Selecione uma ação de backup e clique em **Exibir detalhes**.

Os resultados do backup fornecem os seguintes detalhes:

- Duração

- Notas
- Nome do administrador
- Componentes com backup

Use a barra de pesquisa no canto superior direito da página **Histórico** para procurar um backup específico. Por exemplo: você pode procurar backups feitos por um administrador específico ou feitos em um dia específico.

Backup e Restauração usando a ferramenta de Configuração Automatizada

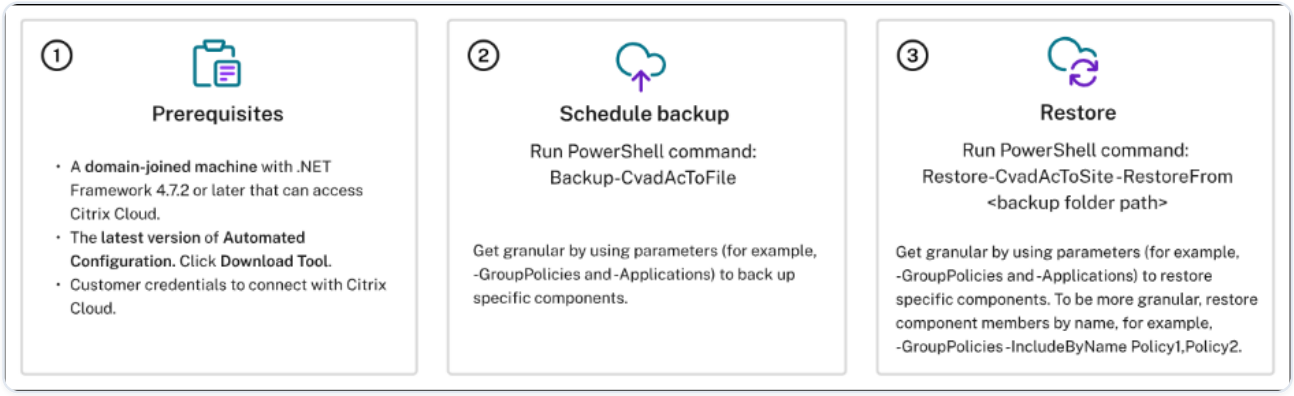
A ferramenta de Configuração Automatizada permite que você faça backups sob demanda e agendados nos seguintes ambientes:

- Citrix Aplicativos Virtuais e Desktops™
- DaaS

A ferramenta de Configuração Automatizada pode ser usada para o seguinte:

- Backup e restauração (backups sob demanda e agendados)
- Migração (backups sob demanda)

Ferramenta de Configuração Automatizada para migração



Citrix Aplicativos Virtuais e Desktops

PRÉ-REQUISITOS PARA FAZER BACKUP DE SUAS CONFIGURAÇÕES

- Todas as versões do Citrix Virtual Apps and Desktops.
- Uma máquina para executar o Auto Config. Este dispositivo pode ser:
  - Um delivery controller™
  - Uma máquina ingressada no domínio com .NET Framework 4.7.2 ou posterior e o SDK do Citrix PowerShell. Para o Citrix PowerShell, você deve instalar o Citrix Studio.

FAZER BACKUP

1. Instale o Automated Configuration. Para obter mais informações, consulte Baixar o Automated Configuration.
2. Clique duas vezes em **Auto-Config**.
3. Na janela do PowerShell, execute o comando `Backup-CvadAcToFile` para exportar todos os componentes. A exportação da sua configuração local não a modifica.

Depois de executar o comando pela primeira vez, o processo cria uma pasta com os arquivos de configuração `.yml` no seguinte local: `%HOMEPATH%\Documents\Citrix\AutoConfig`.

A pasta contém os arquivos de backup da exportação recente, e cada backup anterior é armazenado em uma subpasta.

RESTAURAR

1. Clique duas vezes em **Auto-Config**.
2. Execute o seguinte comando para fazer a restauração:

```
Restore-CvadAcToSite -Environment OnPrem -RestoreFolder <folder path of the backup files>
```

3. Depois de executar o comando, verifique o estado da exportação, e a pasta de log estará disponível em: `%HOMEPATH%\Documents\Citrix\AutoConfig`.
4. Se houver erros ou exceções, consulte a seção **Fixups** no arquivo de log.

DaaS

PRÉ-REQUISITOS PARA FAZER BACKUP DE SUAS CONFIGURAÇÕES

- Um ambiente DaaS com um local de recurso ativo e o Connector instalado.
- Conectividade com sites que acessam o Citrix Cloud. Para obter mais informações, consulte Requisitos de Sistema e Conectividade.

> **Observação**
>
> Você não pode fazer backup do MCS da nuvem usando a Configuração Automatizada.

BACKUP

Faz backup dos seguintes arquivos:

- O arquivo `CustomerInfo.yml` com suas informações de ID do cliente, ID do cliente e chave secreta. Para obter mais informações sobre o processo para recuperar seu ID do cliente, ID do cliente e chave secreta, consulte Gerando o ID do cliente, ID do cliente e chave secreta. Para obter informações sobre como adicionar essas informações ao arquivo `CustomerInfo.yml`, consulte Preenchendo o arquivo de informações do cliente.
- O arquivo `ZoneMapping.yml` com informações que mapeiam seus locais de recurso na nuvem. Para obter mais informações sobre como mapear suas zonas, consulte o Preenchendo o arquivo de mapeamento de zona.
- O arquivo `CvadAcSecurity.yml` com informações sobre conexões de host.

1. Instale a Configuração Automatizada. Para obter mais informações, consulte Instalar a Configuração Automatizada.

> **Observação**
>
> Para backups do DaaS, instale a Configuração Automatizada em uma máquina com acesso à Internet e à qual o administrador também tenha acesso direto.

1. Clique duas vezes em **Auto Config**.
2. Na janela do PowerShell, execute o seguinte comando para fazer um backup: `Export-CvadAcToFile`

Depois de executar o comando pela primeira vez, o processo cria uma pasta com os arquivos de configuração .yml no seguinte local: `%HOMEPATH%\Documents\Citrix\AutoConfig`

A pasta contém os arquivos de backup da exportação recente, e cada backup anterior é armazenado em uma subpasta.

RESTAURAR

1. Clique duas vezes em **Auto Config**.
2. Na janela do PowerShell, execute o seguinte comando para fazer a restauração:

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

3. Após executar o comando, verifique o estado da exportação, e você pode localizar a pasta de log em `%HOMEPATH%\Documents\Citrix\AutoConfig`.
4. Se houver erros ou exceções, consulte a seção **Fixups** no arquivo de log.

Migração granular

> **Nota**
>
> Para obter mais informações sobre a ordem de migração de componentes, consulte Ordem de Migração de Componentes.

RESTAURAR COMPONENTES INTEIROS

Para restaurar um componente, você deve selecionar um ou mais parâmetros.

Por exemplo, para restaurar o grupo de entrega inteiro e os componentes do catálogo de máquinas, execute o seguinte comando:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups
-MachineCatalogs
```

RESTAURAR MEMBROS DO COMPONENTE

Para restaurar um ou mais membros do componente, use o recurso `IncludeByName`. Você deve invocar o cmdlet `Restore` com o parâmetro `Restorefolder` juntamente com o componente selecionado e a lista de inclusão.

Por exemplo, para restaurar duas políticas de grupo de um backup:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -GroupPolicies
-IncludeByName Policy1,Policy2
```

RESTAURAR CONFIGURAÇÃO COMPLETA DO SITE NA NUVEM

Para restaurar todos os componentes ou o site completo na nuvem, execute o seguinte comando:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

Ferramenta de Configuração Automatizada para backup e restauração

Os comandos da ferramenta de Configuração Automatizada acionam as APIs de backup e restauração que o Studio usa.

Os cmdlets `BckRstr` registram no console. Pastas com informações de log não são criadas em `\Documents\Citrix\AutoConfig`.

> **Nota:**
>
> Os pré-requisitos para fazer backup de suas configurações no Citrix Virtual Apps and Desktops e no Citrix DaaS™ são os mesmos da ferramenta de Configuração Automatizada na sessão do PowerShell.

Backup

Para iniciar uma nova ação de backup no Delivery Controller, execute `New-BckRstrBackup` na janela do PowerShell.

Restaurar

Para restaurar membros de um único componente de um backup existente, execute `Restore-BckRstrBackups` na janela do PowerShell.

Para a lista completa de comandos, consulte cmdlets da ferramenta de configuração automatizada para backup e restauração.

Práticas recomendadas para backup e restauração

Este artigo fornece várias recomendações que podem ajudar a planejar melhor o backup e a restauração.

CATEGORIA	MELHOR PRÁTICA
Agendamento de backups	Configure um agendamento de backup padrão, que pode ser executado diariamente, semanalmente ou mensalmente, com base na frequência com que você espera que a configuração do seu site mude. Defina este agendamento padrão para um período menos ativo, possivelmente fins de semana ou meia-noite. Para obter informações sobre backups agendados, consulte Criar backups agendados.

CATEGORIA	MELHOR PRÁTICA
	Se você tiver vários agendamentos de backup definidos que podem ser executados no mesmo dia, use a guia **Configurações** no nó **Backup e Restauração** para redefinir o limite para um backup por dia.
Gerenciando backups	Sempre fixe os backups de cópia dourada para que sejam retidos quando o limite de 30 backups for atingido. Clique com o botão direito do mouse em um backup para fixar o backup selecionado.

Perguntas frequentes

Administradores personalizados podem fazer backup e restauração?

Não. A funcionalidade de backup e restauração é limitada a administradores com direitos totais.

Podemos fazer backup de componentes seletivos?

Não. Atualmente, os backups sob demanda e agendados fazem backup de toda a configuração do site. Os componentes têm várias dependências e pré-requisitos. Para garantir a resolução adequada dessas dependências, você pode fazer backup dos componentes na íntegra. No entanto, você pode restaurar componentes seletivos.

Podemos baixar backups?

Atualmente, use o ACT para baixar backups do seu site DaaS. Você pode baixar o ACT em Configuração Automatizada para Virtual Apps and Desktops.

Podemos fazer backup e restaurar catálogos MCS?

Atualmente, não podemos fazer backup e restaurar catálogos MCS. Você pode usar o ACT para fazer backup dos seus catálogos MCS e importá-los para outro site.

Migrar configuração para Citrix Cloud™

A Ferramenta de Configuração Automatizada (ACT) permite a migração da configuração do Citrix Virtual Apps and Desktops™ (políticas, aplicativos, catálogos, funções de administrador, escopos e outros) de um ou mais sites locais para o Citrix DaaS hospedado no Citrix Cloud. Ela também pode ser usada para migrar informações entre diferentes regiões ou locatários da nuvem.

Esta ferramenta descobre e exporta um ou mais sites locais como uma coleção de arquivos de configuração, que você pode editar opcionalmente. A configuração desses arquivos pode então ser importada para o Citrix DaaS. A migração é feita em etapas, executando a ferramenta várias vezes, permitindo que você alcance facilmente o estado de configuração desejado.

O ACT não é apenas uma ferramenta de migração única. Você pode usá-lo para gerenciar suas operações diárias na nuvem, como:

- Automatizar a transferência de contas de nuvem de teste ou de estágio para contas de nuvem de produção
- Fazer backup e restaurar sua configuração
- Dividir um ambiente de nuvem em várias nuvens

O vídeo a seguir de *2 minutos* oferece um tour rápido pela Configuração Automatizada.

<iframe src="https://www.youtube.com/embed/uyQ9o2L1DXQ" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Para obter informações adicionais sobre a Configuração Automatizada, consulte Prova de Conceito: Ferramenta de Configuração Automatizada na Tech Zone.

Para uma análise mais aprofundada sobre como mover sua implantação e preparar sua configuração local para migração, consulte Guia de Implantação: Migrando Citrix Virtual Apps and Desktops do local para o Citrix Cloud na Tech Zone.

Limitações conhecidas

- Os catálogos de máquinas provisionados por meio do Machine Creation Services™ têm considerações especiais. Para obter mais informações sobre o MCS, consulte Entender a migração de catálogos provisionados pelo Machine Creation Services.

Pré-requisitos para migrar sua configuração

Para *exportar* sua configuração do Citrix Virtual Apps and Desktops, você precisa:

- Citrix Virtual Apps and Desktops: versão atual e seu predecessor imediato ou Citrix Virtual Apps and Desktops, XenApp e XenDesktop® LTSRs: todas as versões
- Uma máquina ingressada no domínio com .NET Framework 4.7.2 ou posterior e o SDK do Citrix PowerShell. Isso é instalado automaticamente no Delivery Controller. (Para executar em uma máquina diferente do Delivery Controller local, o Citrix Studio deve ser instalado, pois o Studio instala os snap-ins corretos do PowerShell. O instalador do Studio pode ser encontrado na mídia de instalação do Citrix Virtual Apps and Desktops.)

Para *importar* sua configuração para o Citrix DaaS, você precisa:

- Uma máquina com acesso ao Citrix Cloud. Esta não precisa ser um Delivery Controller™ ou uma máquina ingressada no domínio.
- Citrix DaaS provisionado.
- Um local de recurso ativo com o Connector instalado e ingressado no mesmo domínio da configuração local.
- A conectividade com sites que acessam o Citrix Cloud deve ser permitida e disponível. Para obter mais informações, consulte Requisitos de Sistema e Conectividade.

> **Nota:**
>
> A Configuração Automatizada não pode ser instalada em um sistema Cloud Connector.

Etapas principais

1. Baixe a Ferramenta de Configuração Automatizada e revise os requisitos do sistema. Consulte Baixar Configuração Automatizada.
2. Preencha o arquivo `CustomerInfo.yml` com seus valores de `CustomerName`, `CustomerID` e `SecretKey` gerados no portal do Citrix Cloud. Consulte Gerar o ID do cliente, ID do cliente e chave secreta e Preencher o arquivo de informações do cliente.
3. Se o site local contiver várias zonas, atualize o arquivo `ZoneMapping.yml` para mapear as zonas para os locais de recurso do Citrix DaaS. Consulte Preencher o arquivo de mapeamento de zona.
4. Se o site contiver várias conexões de hospedagem, atualize o arquivo `CvadAcSecurity.yml` com as informações de conexão para cada tipo de host que está sendo migrado para o Citrix DaaS. Se houver apenas uma única conexão de host, atualize o arquivo `CvadACSecurity.yml` com as informações de conexão para a conexão de host. Consulte Atualizar o arquivo de segurança para conexões de host.
5. Abra o ACT e exporte seu site local usando o comando `Export-CvadAcToFile`. Consulte Objetos de migração suportados para a lista de componentes suportados para migração. Para obter informações sobre as etapas para exportar, consulte Exportar configuração local.
6. Importe componentes em estágios usando o comando `Merge-CvadAcToSite`. Alternativamente, migre o site inteiro de uma vez. Certifique-se de migrar os componentes na

ordem listada em Ordem de migração de componentes. Para obter informações sobre as etapas de importação, consulte Executar uma importação.

7. Ative o site da nuvem. Consulte Ativar sites.

Baixar Configuração Automatizada

Baixe e instale a ferramenta de Configuração Automatizada em Downloads da Citrix.

Atualizar Configuração Automatizada

Para evitar erros de funcionalidade, use sempre a versão mais recente disponível do ACT.

Para saber a versão da sua ferramenta, faça o seguinte:

1. Clique duas vezes no ícone **Auto Config**. Uma janela do PowerShell é exibida.
2. Execute o seguinte comando para verificar o número da sua versão.

```
Get-CvadAcStatus
```

3. Verifique a versão da sua ferramenta em relação à versão listada em Downloads da Citrix. A versão mais recente da ferramenta está localizada lá.
4. Baixe e instale a versão mais recente da ferramenta. Você *não* precisa desinstalar a versão antiga para atualizar a Configuração Automatizada.

Nota:

Ao executar cmdlets para acessar a nuvem na Configuração Automatizada, a ferramenta o alerta quando há uma versão mais recente disponível para download. Para obter mais informações sobre cmdlets, consulte Cmdlets da ferramenta de Configuração Automatizada.

Gerar o ID do cliente, ID do cliente e chave secreta

Para migrar o site local para o Citrix DaaS, preencha o arquivo `CustomerInfo.yml` com o ID do cliente, ID do cliente e chave secreta do portal do Citrix Cloud.

Para recuperar o ID do Cliente:

1. Faça login na sua conta Citrix Cloud e selecione o cliente.
2. Clique no ícone da grade e selecione **Identity and Access Management**.

3. navegar para **API access > Secure clients**. O ID do cliente é exibido na página.

Para recuperar o ID do Cliente e a Chave Secreta:

1. Na página **Secure clients**, insira um nome na caixa. Este nome é usado para diferenciar entre vários IDs de cliente e chaves secretas.
2. Clique em Create Client para criar o ID do cliente e a chave secreta.
3. Copie o ID do cliente e a chave secreta para um local seguro e baixe o arquivo `.csv` contendo essas informações. Use o arquivo `.csv` para preencher o arquivo `CustomerInfo.yml`.

> **Nota:**
>
> - O ID do cliente e a chave secreta não expiram. Se forem comprometidos, remova-os imediatamente usando o ícone **Lixeira** e crie novos.
> - A chave secreta não pode ser recuperada se for perdida ou esquecida; um novo ID de cliente e chave secreta devem ser criados.

Preencher arquivo de informações do cliente

O arquivo `CustomerInfo.yml` elimina a necessidade de fornecer parâmetros de informações do cliente toda vez que o cmdlet é executado. Qualquer uma das informações do cliente pode ser substituída usando parâmetros do cmdlet.

Use o cmdlet `New-CvadAcCustomerInfoFile` para criar o arquivo `CustomerInfo.yml`.

> **Importante:**
>
> Não edite manualmente o arquivo `CustomerInfo.yml`. Isso pode causar erros de formatação inadvertidos.

> O cmdlet `New-CvadAcCustomerInfoFile` tem os seguintes parâmetros obrigatórios.

- CustomerId – ID do cliente.
- ClientId – ID do cliente criado no Citrix Cloud.
- Secret – segredo do cliente criado no Citrix Cloud.

Exemplo:

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId
6813EEA6-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaaw==
```

Você também pode criar o `CustomerInfo.yml` usando o parâmetro `SecurityCsvFileSpec` que aponta para o arquivo `security.csv` baixado. Você também deve especificar o CustomerId.

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:
\Users\my_user_name\downloads/security.csv -CustomerId markhof123
```

Use o cmdlet `Set-CvadAcCustomerInfoFile` para atualizar o arquivo `CustomerInfo.yml`. Este cmdlet altera apenas o Client ID.

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

A seguir, um exemplo do arquivo CustomerInfo.yml.

```
# Created/Updated on 2020/01/29 16:46:47

CustomerId: ‘markhof123’

ClientId: ‘6713FEA6-46CC-4F8A-BC71-539F2DDK5384’

Secret: ‘TwBLaaabbbaaaaaaaaaaw==’

Environment: Production

AltRootUrl: ‘’

StopOnError: False

AlternateFolder: ‘’

Locale: ‘en-us’

Editor: ‘C:\Program Files\Notepad++\notepad++.exe’

Confirm: True
```

```
DisplayLog: True
```

Preencher arquivo de mapeamento de zona

Uma zona local é o equivalente ao local de recurso na nuvem. Ao contrário de outros componentes do site, você não pode importar a zona local para a nuvem automaticamente. Em vez disso, ela deve ser mapeada manualmente usando o arquivo `ZoneMapping.yml`. Falhas de importação podem ocorrer se o nome da zona não estiver associado a um nome de local de recurso existente.

Se os sites locais tiverem apenas uma zona e os sites na nuvem tiverem apenas um local de recurso, a ferramenta de Configuração Automatizada fará a associação correta, eliminando a necessidade de gerenciar manualmente o arquivo `ZoneMapping.yml`.

No entanto, se os sites locais tiverem várias zonas ou os sites na nuvem tiverem vários locais de recurso, atualize manualmente o arquivo `ZoneMapping.yml` para refletir o mapeamento correto das zonas locais para os locais de recurso na nuvem.

O arquivo `ZoneMapping.yml` está localizado em `%HOMEPATH%\Documents\Citrix\AutoConfig`. O conteúdo do arquivo `.yml` é um dicionário com o nome da zona como chave e o nome do local de recurso como valor.

Por exemplo, um site local do Citrix Virtual Apps and Desktops com uma zona primária chamada "Zone-1" e uma zona secundária chamada "Zone-2" é migrado para uma implantação do Citrix DaaS com dois locais de recurso na nuvem recém-criados chamados "Cloud-RL-1" e "Cloud-RL-2". Neste caso, o ZoneMapping.yml seria configurado da seguinte forma:

```
            Zone-1: Cloud-RL-1



            Zone-2: Cloud-RL-2
```

Observação:

Adicione um espaço entre os dois pontos e o nome do local do recurso. Se forem usados espaços no nome da zona ou do local do recurso, coloque o nome entre aspas.

Atualizar o arquivo de segurança para conexões de host

As conexões de host e seus hipervisores associados podem ser exportados e importados usando o ACT.

Adicionar um hipervisor a uma conexão de host requer informações de segurança específicas para o tipo de hipervisor. Essas informações não podem ser exportadas do site local por questões de segurança. Você deve fornecer as informações manualmente para que a Configuração Automatizada possa importar com sucesso as conexões de host e os hipervisores para o site da nuvem.

O processo de exportação cria o arquivo `CvadAcSecurity.yml` em `%HOMEPATH%\Documents\Citrix\AutoConfig` contendo espaços reservados para cada item de segurança necessário para o tipo de hipervisor específico. Você deve atualizar o arquivo `CvadAcSecurity.yml` antes de importar para o site da nuvem. As atualizações do administrador são mantidas em várias exportações, com novos espaços reservados de segurança adicionados conforme necessário. Os itens de segurança nunca são removidos. Para obter mais informações, consulte Atualizar manualmente o arquivo CvadAcSecurity.yml

```
HostConn1:

ConnectionType: XenServer®

UserName: root

PasswordKey: rootPassword

HostCon2:

ConnectionType: AWS

ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH

SecretKey: TwBLaaaaaaaaaaaaaaaaw==

Region: East
```

Informações de segurança por hipervisor

A seguir, são listadas as informações de segurança necessárias para cada tipo de hipervisor.

- XenServer, Hyper-V, VMware

    - Nome de Usuário
    - Senha em texto claro
- Microsoft Azure
    - ID da Assinatura
    - ID do Aplicativo
    - Segredo do Aplicativo
- AWS
    - ID da Conta de Serviço
    - Segredo do Aplicativo
    - Região

Considerações especiais de segurança

Todas as informações de segurança são inseridas como texto simples. Se o texto simples não for recomendado, as conexões de host e os hipervisores associados podem ser criados manualmente usando o **Studio**. As conexões de host e os nomes dos hipervisores devem corresponder exatamente aos seus equivalentes locais para que os catálogos de máquinas que usam as conexões de host possam ser importados com sucesso.

Exporte sua configuração local do Citrix Virtual Apps and Desktops

Usando um comando `export` PowerShell, você pode exportar sua configuração local existente e obter os arquivos `.yml` necessários. Esses arquivos são usados para importar a configuração desejada para o Citrix Cloud.

Objetos de migração suportados

A Configuração Automatizada suporta a movimentação da configuração dos seguintes componentes:

- Tags
- Administrador Delegado
    - Escopos
    - Funções
- Conexões de Host

    - Um Único Pool de Recursos
    - Escopos de Administrador
- Catálogos de Máquinas
    - Escopos de Administrador
    - Máquinas
    - Acesso Remoto a PC, Físico, Agrupado, Provisionado, MCS, Atribuído
- StoreFront™
- Grupos de Entrega
    - Política de Acesso
    - Associação de Escopo de Administrador
    - Política de Acesso a Aplicativos
    - Política de Atribuição
    - Política de Direitos/Desktop
    - Agendamentos de Energia
    - Persistência de Sessão
    - Pré-lançamento de Sessão
    - Agendamentos de Reinicialização
    - Tags
- Grupos de Aplicativos
    - Associação de Escopo de Administrador
    - Grupos de Entrega
    - Usuários e Grupos
- Aplicativos
    - Pastas de Aplicativos
    - Ícones
    - Aplicativos
    - FTAs Configuradas pelo Broker
    - Tags

- Políticas de Grupo
- Preferências de Zona do Usuário

Exportar configuração local

1. Clique duas vezes no ícone **Auto Config**. Uma janela do PowerShell é exibida.
2. Execute o seguinte comando para exportar todos os componentes. A exportação da sua configuração local *não* a altera de forma alguma.

```
Export-CvadAcToFile
```

Depois de executar qualquer cmdlet pela primeira vez, uma pasta de exportação com os arquivos de configuração `.yml` e logs é criada. A pasta está em `%HOMEPATH%\Documents\Citrix\AutoConfig`. Cada exportação sucessiva cria uma subpasta. A pasta pai `%HOMEPATH%\Documents\Citrix\AutoConfig` sempre contém os arquivos exportados da exportação mais recente.

> **Nota:**

> Se a Configuração Automatizada não estiver instalada no Delivery Controller, execute `import-module Citrix.AutoConfig.Commands` antes de usar a ferramenta via PowerShell. Esta etapa não é necessária se você abrir a Configuração Automatizada usando o ícone **Auto Config**.

> Se você encontrar quaisquer erros ou exceções, consulte a seção **Fixups** no arquivo de log.

Importar sua configuração para o Citrix DaaS

> **Importante:**

> - Ao migrar uma implantação local para a nuvem, certifique-se de que os GPOs de domínio e UO que contêm as configurações do Citrix sejam migrados para a nuvem. O Citrix Web Studio™ não oferece suporte a GPMC e, portanto, os GPOs de domínio e UO não são visíveis no Web Studio. O mecanismo de política do Citrix impõe os GPOs de domínio e UO em VDAs e usuários que estão nos domínios e UOs. Após o login em um

> VDA, um usuário pode ver que as políticas dos GPOs de domínio e UO são aplicadas à sua sessão. No entanto, os administradores não conseguem ver essas políticas e configurações, o que pode levar a confusões.

Ordem de migração de componentes

Os componentes e suas dependências estão listados aqui. As dependências de um componente devem estar em vigor antes que ele possa ser importado ou mesclado. Se uma dependência estiver ausente, isso pode fazer com que o comando de importação ou mesclagem falhe. A seção **Fixups** do arquivo de log mostra as dependências ausentes se uma importação ou mesclagem falhar.

1. Tags
    - Sem pré-dependências
2. Administrador Delegado
    - Sem pré-dependências
3. Conexões de Host
    - Informações de Segurança em CvadAcSecurity.yml
4. Catálogos de Máquinas
    - Máquinas presentes no Active Directory
    - Conexões de Host
    - Tags
5. StoreFront
6. Grupos de Entrega
    - Máquinas presentes no Active Directory
    - Usuários presentes no Active Directory
    - Catálogos de Máquinas
    - Tags
7. Grupos de Aplicativos
    - Grupos de Entrega

- Tags

8. Aplicativos
   - Grupos de Entrega
   - Grupos de Aplicativos
   - Tags
9. Políticas de Grupo
   - Grupos de Entrega
   - Tags
10. Preferências de Zona do Usuário

Executar uma importação

1. Clique duas vezes no ícone **Auto Config**. Uma janela do PowerShell é exibida.
2. Execute o seguinte comando para importar todos os componentes.

```
Merge-CvadAcToSite
```

Verifique o estado esperado com o novo estado atual. Várias opções de importação controlam se os resultados da importação são idênticos ou um subconjunto do site local.

Depois de executar o cmdlet, uma pasta de exportação com os arquivos de configuração `.yml` e logs é criada. A pasta está em `%HOMEPATH%\Documents\Citrix\AutoConfig`.

Se você encontrar erros ou exceções, consulte a seção **Fixups** no arquivo de log.

> **Nota:**

> Se a Configuração Automatizada não estiver instalada no Delivery Controller, execute `import-module Citrix.AutoConfig.Commands` antes de usar a ferramenta via PowerShell. Esta etapa não é necessária se você abrir a Configuração Automatizada usando o ícone **Auto Config**.

> Para reverter para a sua configuração original do Citrix DaaS, consulte Fazer backup da sua configuração do Citrix DaaS.

Entender a operação de importação

O processo de importação foi projetado para realizar atualizações com precisão, executar apenas as atualizações necessárias e verificar se todas as atualizações foram feitas corretamente. As etapas a seguir são realizadas em todas as operações de importação:

1. Ler o arquivo .yml exportado (estado esperado).
2. Ler a nuvem (estado atual).
3. Fazer backup do estado da nuvem pré-importação para arquivos .yml (o pré-backup pode ser restaurado se necessário).
4. Avaliar as diferenças entre o estado esperado e o estado atual. Isso determina quais atualizações devem ser feitas.
5. Fazer as atualizações.
6. Reler a nuvem (novo estado atual).
7. Fazer backup do estado da nuvem pós-importação para arquivos .yml (o pós-backup pode ser restaurado se necessário).
8. Comparar o novo estado atual com o estado esperado.
9. Relatar os resultados da comparação.

Migração granular

> **Importante:**

> Para obter mais informações sobre a ordem de migração de componentes, consulte Ordem de migração de componentes.

> Você pode migrar seletivamente apenas componentes ou até mesmo apenas nomes de componentes.

- Os parâmetros de componente suportados incluem `MachineCatalogs`, `Tags` e muito mais.
- Os parâmetros de nome de componente suportados incluem os parâmetros `IncludeByName` e `ExcludeByName`, e outros.

Para obter mais informações sobre parâmetros e como usá-los, consulte Parâmetros de migração granular.

Ativar sites

O controlador de entrega em sites locais e na nuvem controla recursos como a intermediação de desktops, aplicativos e reinicialização de máquinas. Problemas ocorrem quando um conjunto comum de recursos é controlado por dois ou mais sites. Essa situação pode ocorrer ao migrar de um site local para um site na nuvem. É possível que os controladores de entrega locais e na nuvem gerenciem o mesmo conjunto de recursos. Tal gerenciamento duplo pode levar a recursos se tornando indisponíveis e incontroláveis, e pode ser difícil de diagnosticar.

A ativação do site permite controlar onde o site ativo é controlado.

A ativação do site é gerenciada usando o modo de manutenção do grupo de entrega. Os grupos de entrega são colocados em modo de manutenção quando o site está inativo. O modo de manutenção é removido dos grupos de entrega para sites que estão ativos.

A ativação do site não afeta nem gerencia o registro de VDA ou catálogos de máquinas.

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

Todos os cmdlets suportam a `IncludeByName` e `ExcludeByName` filtragem. Este parâmetro permite selecionar quais grupos de entrega podem ter seu modo de manutenção alterado. Os grupos de entrega podem ser alterados seletivamente conforme necessário.

Importar e transferir o controle para a nuvem

A seguir, uma descrição de alto nível sobre como importar e transferir o controle do site local para o site na nuvem.

1. Exporte e importe o site local para a nuvem. Certifique-se de que o parâmetro `-SiteActive` não esteja presente em nenhum dos cmdlets de importação. O site local está ativo e o site na nuvem inativo. Por padrão, os grupos de entrega do site na nuvem estão em modo de manutenção.
2. Verifique o conteúdo e a configuração da nuvem.
3. Durante o horário de inatividade, defina o site local como inativo. O parâmetro `-SiteActive` deve estar ausente. Todos os grupos de entrega do site local estão em modo de manutenção.
    - `Set-CvadAcSiteActiveStateOnPrem`
4. Defina o site na nuvem como ativo. O parâmetro `-SiteActive` deve estar presente. Nenhum grupo de entrega do site na nuvem está em modo de manutenção.

- `Set-CvadAcSiteActiveStateCloud –SiteActive`

5. Verifique se o site na nuvem está ativo e o site local está inativo.

Transferir o controle de volta para o site local

Para transferir o controle do site na nuvem para o site local:

1. Durante o horário de inatividade, defina o site na nuvem como inativo. Todos os grupos de entrega do site na nuvem estão em modo de manutenção.
   - `Set-CvadAcSiteActiveStateCloud`
2. Defina o site local como ativo. Nenhum grupo de entrega do site local está em modo de manutenção.
   - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

Informações adicionais de ativação do site

- Se nenhuma máquina for gerenciada por energia e não houver agendamentos de reinicialização (o que geralmente significa que também não há conexões de host), todos os grupos de entrega na nuvem podem ser importados como ativos. Adicione `-SiteActive` a `Merge-CvadAcToSite`/`Import-CvadAcToSite` ou execute `Set-CvadAcSiteActiveStateCloud -SiteActive` após a importação.
- Se as máquinas forem gerenciadas por energia ou houver agendamentos de reinicialização, um processo diferente é necessário. Por exemplo, ao mudar de on-premises para a nuvem nesta situação, defina o site on-premises como inativo usando `Set-CvadAcSiteActiveStateOnPrem`. Em seguida, defina o site da nuvem como ativo usando `Set-CvadAcSiteActiveStateCloud -SiteActive`.
- Os cmdlets `Set-CvadAcSiteActiveStateCloud` e `Set-CvadAcSiteActiveStateOnPrem` também são usados para reverter o processo. Por exemplo, execute `Set-CvadAcSiteActiveStateCloud` sem o parâmetro `-SiteActive`, e depois execute `Set-CvadAcSiteActiveStateOnPrem` com o parâmetro `-SiteActive`.

Entender a migração de catálogos provisionados pelo Machine Creation Services

> **Nota:**

> Este recurso está disponível apenas nas versões 3.0 e posteriores. Verifique sua versão usando `Get-CvadAcStatus` dentro da Configuração Automatizada.

> Os catálogos do Machine Creation Services (MCS) criam dois tipos diferentes de catálogos:

- Quando as alterações feitas em uma máquina são perdidas ou revertidas (comumente SO de Servidor, onde os aplicativos são publicados) – este é um caso de uso de VDI agrupado / multi-sessão
- Quando as alterações feitas em uma máquina são preservadas após a reinicialização (comumente SO cliente com um usuário dedicado) – este é um caso de uso de VDI estático

O tipo de catálogo pode ser confirmado no nó do catálogo no Citrix Studio e verificando o valor "Dados do usuário:" do catálogo.

> **Nota:**
>
> O MCS não pode ser copiado da nuvem usando a Configuração Automatizada.

Catálogos VDI agrupados / multi-sessão

Catálogos com "Dados do usuário: Descartar" são catálogos VDI agrupados e só podem migrar a imagem principal e a configuração. Nenhuma máquina virtual nesses catálogos é migrada. Isso ocorre porque o ciclo de vida da máquina virtual é mantido pelo site de onde você está importando, o que significa que toda vez que as máquinas são ligadas, seu estado pode mudar. Isso torna a importação impossível, pois os dados de importação para as máquinas virtuais rapidamente ficam dessincronizados.

Ao migrar esses catálogos usando a ferramenta, ela cria metadados do catálogo e inicia a criação da imagem principal, mas nenhuma máquina é importada.

Como este processo pode levar algum tempo para ser criado com base no tamanho da imagem principal, o comando de importação dentro da ferramenta apenas inicia a criação do catálogo MCS e não espera que ele termine. Após a conclusão da importação, monitore o progresso da criação do catálogo usando o Studio na implantação em nuvem.

Uma vez que a imagem principal é criada, você pode provisionar máquinas. Considere as considerações de capacidade, pois você teria capacidade consumida do seu uso local.

Todos os outros objetos (grupos de entrega, aplicativos, políticas e assim por diante) que usam esse catálogo podem ser importados e não precisam esperar pela criação da imagem principal. Quando o catálogo terminar de ser criado, as máquinas podem ser adicionadas ao catálogo importado e, então, os usuários podem iniciar seus recursos.

> **Nota:**
>
> Use os mesmos comandos disponíveis na ferramenta para migrar catálogos e todos os outros objetos.

Catálogos VDI estáticos

> **Nota:**
>
> Como esta operação importa detalhes de baixo nível que são armazenados no banco de dados, este processo deve ser executado a partir de uma máquina com acesso ao banco de dados.

> Os catálogos VDI estáticos migram a imagem principal, as configurações e todas as máquinas virtuais. Ao contrário do caso de uso de VDI agrupado, nenhuma imagem precisa ser criada.

Os VDAs devem ser apontados para o conector para que se registrem na nuvem.

Consulte a seção Ativando sites para tornar o site da nuvem ativo, de modo que o agendamento de reinicialização, o gerenciamento de energia e outros itens sejam controlados pela nuvem.

Uma vez concluída a migração, se você quiser excluir este catálogo do seu site local, você deve selecionar **manter VM e conta AD**. Caso contrário, eles serão excluídos e o site da nuvem ficaria apontando para a VM excluída.

Atualizar tags MCS para detectar recursos órfãos após a migração

Depois de migrar da configuração local para um site na nuvem, ou da sua configuração na nuvem para outro site na nuvem, você deve atualizar as tags de ID do site MCS no caso de VMs persistentes para que os recursos órfãos possam ser detectados corretamente. Para fazer isso,

use o comando PowerShell `Set-ProvResourceTags`. Atualmente, este recurso é aplicável ao Azure.

Os passos detalhados são os seguintes:

1. Atualize as tags de ID do site MCS do novo site Citrix usando o comando PowerShell `Set-ProvResourceTags`. Por exemplo:

   ```
   Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

   Ou,

   ```
   Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

Os detalhes do parâmetro são os seguintes:

- `ProvisioningSchemeUid` ou `ProvisioningSchemeName` é um parâmetro obrigatório.
- `VMName` é um parâmetro opcional. Se nenhum `VMName` for especificado, as tags de todas as VMs deste catálogo de máquinas são atualizadas.
- `VMBatchSize` é um parâmetro opcional para dividir todas as VMs em lotes. Se nenhum `VMBatchSize` for especificado, o valor padrão (10) é aplicado. O intervalo é de 1 a 60.
- `ResourceType` pode ser um dos seguintes:
  - `MachineCatalog`: Para atualizar tags de recursos de catálogo de máquinas.
  - `VirtualMachine`: Para atualizar tags de recursos relacionados à VM.
  - `All`: (ResourceType padrão): Para atualizar tags de recursos de catálogo de máquinas e recursos relacionados à VM.

Mesclar vários sites em um único site

O suporte a vários sites para a Configuração Automatizada oferece um método para mesclar vários sites locais em um único site na nuvem.

O suporte a vários sites adiciona prefixos e sufixos exclusivos aos nomes dos componentes por site local, garantindo a exclusividade do nome depois que vários sites locais são mesclados em um único site na nuvem.

Prefixos e sufixos podem ser atribuídos para cada um dos seguintes componentes por site local.

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`
- `StoreFront`
- `Tag`

Pastas de aplicativos suportam prefixação, sufixação e rerooting. Rerooting adiciona uma pasta de nível superior extra à estrutura de pastas existente de um aplicativo.

Regras de prefixo e sufixo

1. Prefixos e sufixos não podem conter nenhum dos seguintes caracteres especiais: `\ , / ; : # . * ? = < > | ( ) " ' { } [ ]`
2. Prefixos e sufixos podem conter espaços à direita, mas não espaços à esquerda.
3. Prefixos e sufixos devem ser colocados entre aspas duplas para conter espaços à direita.
4. Prefixos e sufixos são aplicados no momento da importação, mesclagem e adição. Os arquivos `.yml` de origem nunca são modificados.
5. O processo de prefixo e sufixo prefixa ou sufixa automaticamente os nomes dos componentes dependentes, quando aplicável. Por exemplo, se os nomes dos catálogos de máquinas forem prefixados com "East", então os grupos de entrega que os referenciam também são prefixados com "East".
6. Se um nome de componente já começar com o prefixo ou sufixo, nenhum prefixo ou sufixo será adicionado. Os nomes dos componentes não podem conter prefixos ou sufixos idênticos duplos.
7. Prefixos e sufixos podem ser usados individualmente ou em combinação.

8. O uso de um prefixo ou sufixo em um componente é opcional.

> **Nota:**
>
> O Studio exibe os componentes em ordem alfabética.

Agrupar componentes por site

Use a prefixação para agrupar visualmente componentes de um único site. Cada site é listado em seu próprio grupo, com a prefixação controlando alfabeticamente a ordenação de diferentes grupos de sites.

Agrupar componentes por nome

Use sufixos para agrupar visualmente componentes com nomes semelhantes de vários sites. Componentes com nomes semelhantes de sites diferentes alternam visualmente.

Arquivo de mapeamento de prefixo e sufixo

A prefixação do site começa com o arquivo `SiteMerging.yml` que contém o mapeamento de prefixo e sufixo do site para um ou mais sites locais. Você pode gerenciar o arquivo `SiteMerging.yml` manualmente ou usando os cmdlets disponíveis listados na seção Cmdlets de mesclagem de vários sites locais.

Exportar site local

A mesclagem não pode começar até que você tenha exportado um site local. Para exportar um site local, consulte Exportar configuração local.

Pasta de destino de exportação central

Os métodos descritos nesta seção colocam várias exportações de site em um local de compartilhamento de arquivos central. O arquivo `SiteMerging.yml`, o arquivo `CustomerInfo.yml` e todos os arquivos de exportação residem nesse local de compartilhamento de arquivos, permitindo que você faça a importação de um único local, independente dos sites locais.

As operações de acesso à nuvem nunca fazem referência aos sites locais ou ao Active Directory, permitindo que você realize operações de acesso à nuvem de qualquer lugar.

Existem dois métodos para fazer isso:

- Compartilhamento de arquivo direto: Para importar, mesclar ou adicionar a partir do compartilhamento de arquivo direto, você deve decidir de qual máquina deseja realizar a operação de acesso à nuvem
- Referência de compartilhamento de arquivo usando `SiteMerging.yml`: Este método usa o membro `SiteRootFolder` do conjunto de prefixos do site e reduz as chances de direcionar a pasta errada ao exportar, importar, mesclar ou adicionar.

Se você não usar um método de compartilhamento de arquivo central, faça a importação, mesclagem ou adição a partir dos Delivery Controllers individuais. Crie e replique o arquivo `SiteMerging.yml` em cada Delivery Controller sendo migrado para a nuvem. O local padrão é `%HOMEPATH%\Documents\Citrix\AutoConfig`. Você deve especificar o parâmetro `-SiteName` para selecionar os prefixos de site corretos.

Compartilhamento de arquivo direto

As operações de exportação, importação, mesclagem e novo/adicionar fornecem um parâmetro para direcionar ou originar uma pasta diferente da pasta padrão, *%HOMEPATH%\Documents\Citrix\AutoConfig*. Os exemplos a seguir usam um compartilhamento de arquivo central em `\\share.central.net` ao qual o administrador já tem acesso, tendo fornecido as credenciais conforme necessário.

Para direcionar a exportação para uma pasta específica do site, use o parâmetro `-TargetFolder`:

Do Delivery Controller™ Leste:

```
mkdir  \\share.central.net\AutoConfig\SiteEast



Export-CvadAcToFile   –TargetFolder   \
\share.central.net\AutoConfig\SiteEast
```

Do Delivery Controller Oeste:

```
mkdir  \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile   –TargetFolder   \
\share.central.net\AutoConfig\SiteWest`
```

Após a conclusão das exportações, crie os arquivos CustomerInfo.yml e SiteMerging.yml e coloque-os em `\\share.central.net\AutoConfig`.

Observação:

Não use o parâmetro `SiteRootFolder` ao criar o SitePrefixes.yml ao usar este método de referência de compartilhamento de arquivo direto.

Para importar, mesclar ou adicionar a partir do compartilhamento de arquivo direto, você deve decidir de qual máquina deseja realizar a operação de acesso à nuvem. As opções incluem:

- Um dos Delivery Controllers locais onde a ferramenta já está instalada.
- A máquina que hospeda o compartilhamento de arquivo.
- Uma máquina diferente.

A Configuração Automatizada deve ser instalada na máquina que acessa a nuvem. Nem o PowerShell SDK local, o Delivery Controller, nem o Active Directory são usados, portanto, os requisitos de execução de acesso à nuvem são mais simples do que os requisitos de exportação.

Para mesclar o Delivery Controller Leste com a nuvem:

```
Merge-CvadAcToSite –SiteName East –SourceFolder  \
\share.central.net\AutoConfig\SiteEast -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

Para mesclar o Delivery Controller Oeste com a nuvem:

```
Merge-CvadAcToSite –SiteName West –SourceFolder  \
\share.central.net\AutoConfig\SiteWest -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

A seguir, um arquivo `SitePrefixes.yml` de exemplo usado no exemplo anterior.

```
East:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"

  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"
```

```
  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "
```

```
  AdminScopeSuffix: ""

  AdminRoleSuffix: ""

  ApplicationAdminSuffix: ""

  ApplicationFolderSuffix: ""

  ApplicationGroupSuffix: ""

  ApplicationUserSuffix: ""

  DeliveryGroupSuffix: ""

  GroupPolicySuffix: ""

  HostConnectionSuffix: ""

  MachineCatalogSuffix: ""

  StoreFrontSuffix: ""

  TagSuffix: ""
```

Referência de compartilhamento de arquivo usando SiteMerging.yml

Este método usa o `SiteRootFolder` membro do conjunto de prefixos do site. Embora mais complexo do que o método de compartilhamento de arquivos direto, este método reduz as chances de direcionar a pasta errada ao exportar, importar, mesclar ou adicionar.

Primeiro, defina o `SiteRootFolder` para cada site no arquivo SiteMerging.yml. Você deve fazer isso no local compartilhado.

```
New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \
\share.central.net\AutoConfig\SiteEast -SitePrefixesFolder  \
\share.central.net\AutoConfig



New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest
-SitePrefixesFolder  \\share.central.net\AutoConfig
```

Neste exemplo, Leste é uma especificação de pasta totalmente qualificada e Oeste é uma especificação de pasta relativa.

Para direcionar a exportação para uma pasta específica do site usando o arquivo SiteMerging.yml:

Do Delivery Controller Leste:

```
mkdir  \\share.central.net\AutoConfig\SiteEast



Export-CvadAcToFile   -SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

Do Delivery Controller Oeste:

```
mkdir  \\share.central.net\AutoConfig\SiteWest



Export-CvadAcToFile   -SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

O cmdlet de exportação usa o local da pasta CustomerInfo.yml para localizar o arquivo SiteMerging.yml. No caso de Leste, o `SiteRootFolder` é totalmente qualificado. Ele é usado como está. No caso de Oeste, o `SiteRootFolder` não é totalmente qualificado. Ele é combinado com o local da pasta CustomerInfo.yml para recuperar um local de pasta totalmente qualificado para Oeste.

Para mesclar o Delivery Controller Leste com a nuvem:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

Para mesclar o Delivery Controller Oeste com a nuvem:

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

A seguir, um arquivo SitePrefixes.yml de exemplo usado no exemplo anterior.

```
  East:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"

  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"
```

```
  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "
```

```
AdminScopeSuffix: ""

AdminRoleSuffix: ""

ApplicationAdminSuffix: ""

ApplicationFolderSuffix: ""

ApplicationGroupSuffix: ""

ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

Mesclar os sites

A Citrix® recomenda realizar as operações na nuvem em etapas e fazer uma revisão completa de cada resultado antes de realizar a próxima operação na nuvem. Por exemplo, se estiver mesclando três sites em um único site na nuvem:

1. Mescle o site inicial com a nuvem usando o valor `SiteName` apropriado.
2. Revise os resultados no Studio.
3. Se os resultados estiverem incorretos, determine o problema e sua causa, corrija-o e execute a mesclagem novamente. Se necessário, remova os componentes da nuvem e comece do zero usando `Remove-CvadAcFromSite` para o componente e membros selecionados. Se os resultados estiverem corretos, continue.
4. Se a mesclagem inicial estiver correta, mescle o segundo site ao site de nuvem único.
5. Repita as etapas 2 e 3.
6. Se a segunda mesclagem estiver correta, mescle o terceiro site ao site de nuvem único.

7. Repita as etapas 2 e 3.
8. Revise os recursos da perspectiva do usuário e verifique se a visualização está no estado desejado.

Remover um componente usando o prefixo do site

Você pode remover seletivamente componentes de site único usando o prefixo no parâmetro `-IncludeByName` do cmdlet `Remove-CvadAcFromSite`. No exemplo a seguir, os grupos de entrega do West Delivery Controller não estão corretos. Para remover os grupos de entrega apenas para o site Oeste:

```
Remove-CvadAcFromSite   –DeliveryGroups   –IncludeByName “Western *”
```

Para remover todos os componentes Oeste, execute os seguintes cmdlets em ordem.

`Remove-CvadAcFromSite –GroupPolicies –IncludeByName “Western *”`

`Remove-CvadAcFromSite –Applications –IncludeByName “Western *”`

`Remove-CvadAcFromSite – ApplicationGroups –IncludeByName “Western *”`

`Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”`

`Remove-CvadAcFromSite –MachineCatalogs –IncludeByName “Western *”`

`Remove-CvadAcFromSite –HostConnections –IncludeByName “Western *”`

`Remove-CvadAcFromSite –Tags –IncludeByName “Western *”`

Para remover políticas de grupo dos componentes Leste, use o sufixo:

```
Remove-CvadAcFromSite   –GroupPolicies   –IncludeByName “*_east”
```

Migrar de nuvem para nuvem

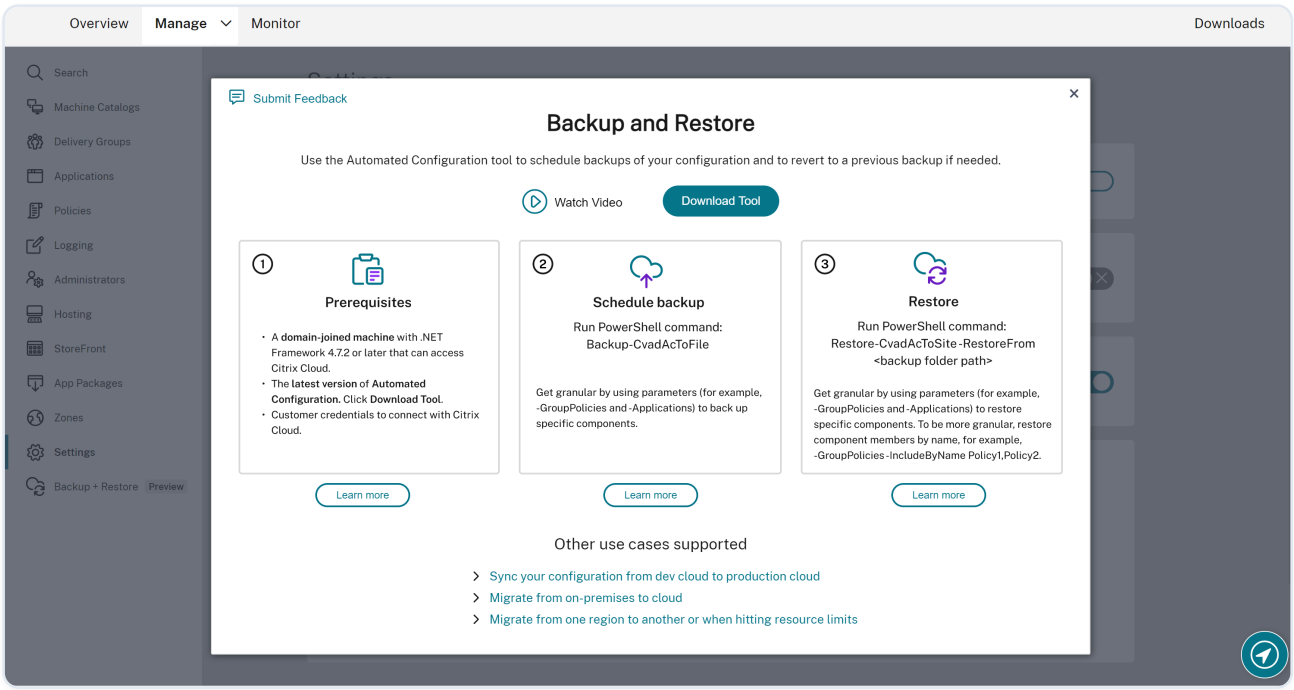
A Configuração Automatizada permite automatizar a movimentação da sua configuração de nuvem para outro site de nuvem ou restaurar o seu próprio site de nuvem.

O uso da Configuração Automatizada pode resolver muitos casos de uso:

- Sincronizar seu site de teste ou estágio para produção
- Fazer backup e restaurar sua configuração

- Atingir limites de recursos
- Migrar de uma região para outra

No Studio no Citrix Cloud™, consulte o nó Backup e Restauração para obter informações sobre a Configuração Automatizada e como ela pode ser usada para migrar sua configuração de nuvem para nuvem.



Pré-requisitos para migrar sua configuração

Para fazer backup e restaurar sua configuração, você precisa:

- Citrix DaaS™ provisionado.
- Um local de recurso ativo com o Connector instalado.
- A conectividade com sites que acessam o Citrix Cloud deve ser permitida e disponível. Para obter mais informações, consulte Requisitos de Sistema e Conectividade.

> **Nota:**
>
> O MCS não pode ser copiado da nuvem usando a Configuração Automatizada.

Faça backup da sua configuração do Citrix DaaS

Requisitos

Faça o seguinte antes de fazer backup da sua configuração do Citrix DaaS:

1. Preencha o arquivo `CustomerInfo.yml` com seu ID de cliente, ID de cliente e as informações da chave secreta incluídas. Para obter mais informações sobre como recuperar seu ID de cliente, ID de cliente e chave secreta, consulte Gerar o ID de cliente, ID de cliente e chave secreta. Para obter informações sobre como adicionar essas informações ao arquivo `CustomerInfo.yml`, consulte Preencher arquivo de informações do cliente.

Ao executar os comandos de backup, o `CustomerInfo.yml` deve conter os detalhes do cliente do site de origem de onde você está fazendo o backup.

Ao executar os comandos de restauração, o `CustomerInfo.yml` deve conter os detalhes do cliente do site de destino para onde você está restaurando as configurações.

1. Preencha o arquivo `ZoneMapping.yml` com informações que mapeiam seus locais de recurso na nuvem. Para obter mais informações sobre como mapear suas zonas, consulte Preencher arquivo de mapeamento de zona.
2. Se você tiver conexões de host, deverá inserir as informações correspondentes no arquivo `CvadAcSecurity.yml`. Consulte Atualizar o arquivo de segurança para conexões de host

Etapas para fazer backup da sua configuração do Citrix DaaS

1. Instalar Configuração Automatizada.

> **Nota:**
>
> Para migração de nuvem para nuvem, a Configuração Automatizada pode ser instalada em uma máquina com acesso à internet à qual o administrador tenha acesso direto.

2. Clique duas vezes no ícone **Auto Config**. Uma janela do PowerShell é exibida.
3. Execute o seguinte comando para fazer um backup.

```
Backup-CvadAcToFile
```

Depois de executar qualquer cmdlet pela primeira vez, uma pasta de exportação com os arquivos de configuração `.yml` e logs é criada. A pasta está em `%HOMEPATH%\Documents\Citrix\AutoConfig`.

Se você encontrar quaisquer erros ou exceções, consulte a seção **Fixups** no arquivo de log.

Restaurar sua configuração para o Citrix DaaS

1. Clique duas vezes no ícone **Auto Config**. Uma janela do PowerShell é exibida.
2. Execute o seguinte comando para fazer uma restauração.

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

Verifique o estado esperado com o novo estado atual.

Depois de executar o cmdlet, uma pasta de exportação com os arquivos de configuração `.yml` e logs é criada. A pasta está em *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Se você encontrar quaisquer erros ou exceções, consulte a seção **Fixups** no arquivo de log.

O processo de backup e restauração protege você contra alterações ou corrupção não intencionais na configuração do site da nuvem. Embora a Configuração Automatizada faça backups cada vez que uma alteração é feita, este backup reflete o estado da configuração do site da nuvem antes das alterações. Proteger-se exige que você faça backup periodicamente da configuração do seu site da nuvem e a salve em um local seguro. Se uma alteração indesejável ou corrupção ocorrer, o backup pode ser usado para corrigir a alteração ou corrupção em um nível de configuração de site granular ou completo.

Migração granular

> **Importante:**
>
> Para obter mais informações sobre as ordens de migração de componentes, consulte Ordem de migração de componentes.

Restaurar todos os componentes

A restauração de um componente envolve a seleção de um ou mais parâmetros de componente.

Para restaurar o:

- grupo de entrega inteiro e componentes do catálogo de máquinas
- configuração completa do site na nuvem

siga este exemplo:

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

Restaurar membros do componente

A restauração de um ou mais membros do componente usa o recurso `IncludeByName`. O cmdlet `Restore` é invocado com o parâmetro `RestoreFolder` juntamente com o componente único selecionado e a lista de inclusão.

Para restaurar duas políticas de grupo de um backup, siga este exemplo:

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

```
-GroupPolicies -IncludeByName   Policy1,Policy2
```

```
-DeliveryGroups -MachineCatalogs`
```

Ativar sites

A ativação do site permite controlar qual site está ativo e gerencia seus recursos. Para obter mais informações, consulte Ativar sites.

Migrar configurações da Nuvem para ambientes locais

Este artigo descreve o backup e a migração de suas configurações da Nuvem para sites locais.

Pré-requisitos para migrar sua configuração

- Ambiente local do Citrix Virtual Apps and Desktops™ com pelo menos um VDA registrado.
- Ambiente local do Citrix Virtual Apps and Desktops executando uma das seguintes versões:
  - A versão mais recente do Long-Term Service Release (LTSR) - 2402.
  - Qualquer uma das versões do Current Releases (CR) - 2308, 2311.
- Execute os comandos da ferramenta de Configuração Automatizada (ACT) em uma máquina ingressada no domínio com a versão .Net 4.7.2 ou superior.
- Uma máquina com o Citrix PowerShell SDK. O PowerShell SDK está disponível no instalável do Citrix Delivery Controller™.

Observação:

- Se você estiver executando o ACT em uma máquina diferente, ela deve estar ingressada no domínio e o Studio deve ter os snap-ins corretos do PowerShell instalados. Para obter o instalador, acesse o site de downloads do Citrix Virtual Apps and Desktops.
- No site local, recomendamos que o ACT seja instalado no DDC. O ACT pode ser iniciado através do ícone da área de trabalho.
- Se o ACT for destinado a ser usado a partir da janela padrão do Powershell, então execute o seguinte comando: `Import-Module Citrix.AutoConfig.Commands`

O ACT não faz parte do caminho do PowerShell do sistema, portanto, deve ser importado explicitamente.

Etapas principais

Siga as instruções para concluir a migração de suas configurações da nuvem para o local:

1. Fazer backup da configuração da nuvem.
2. Modificar arquivos YML.
3. Importar configurações para o local.

Fazer backup da configuração da nuvem

1. Instale o **Automated Configuration**.
2. Clique duas vezes no ícone **Auto Config**. Uma janela do PowerShell é exibida.
3. Execute `New-CvadAcCustomerInfoFile` para criar um arquivo **CustomerInfo.yml**. Para obter mais informações, consulte Preencher arquivo de informações do cliente.
4. Execute o comando `Backup-CvadAcToFile` para fazer um backup de suas configurações da nuvem.

   Nota:

- Depois de executar qualquer cmdlet pela primeira vez, uma pasta de backup com os arquivos de configuração .yml e logs é criada. A pasta está em `%HOMEPATH%\Documents\Citrix\AutoConfig`.
- Se você encontrar erros ou exceções, consulte a seção **Fixups** no arquivo de log.
- Backup-CvadToFile não oferece suporte aos parâmetros `IncludeByName` ou `ExcludeByName`.

Importante:

A Citrix recomenda fazer backup de todos os componentes juntos.

Modificar arquivos YML

Modifique os arquivos `.yml` localizados em `%HOMEPATH%\Documents\Citrix\AutoConfig` para incluir os detalhes locais, conforme descrito na tabela a seguir:

ARQUIVO YML	PARÂMETRO	DESCRIÇÃO	EXEMPLOS
CustomerInfo.yml	Ambiente	Altere o Ambiente para OnPrem. O valor do parâmetro de ambiente diferencia maiúsculas de minúsculas.	
ZoneMapping.yml	DaaS:CVAD	Mapeie os locais dos seus recursos na nuvem para as suas zonas locais.	Deve ser zonas antigas:novas
CvadAcSecurity.yml	Hypervisor: ConnectionType: ‘ ‘ Username: ‘ ’ Password: ‘ ‘	Adicione o nome de usuário e as senhas do hipervisor.	Se o hipervisor for XenServer,XenServer: ConnectionType: ‘XenServer’ Username: ‘root’ Password: ‘ ‘

Importar configurações para o local

1. Execute um dos seguintes comandos em seu site local com base em seus requisitos:

   a. `Merge-CvadAcToSite` - se houver um site local em execução e você quiser mesclar as configurações da Nuvem a ele.

   b. `Import-CvadAcToSite -Environment OnPrem` - Se as configurações locais não estiverem disponíveis e você estiver importando as configurações da Nuvem para criar uma.

> **Importante:**
>
> A Citrix recomenda importar um componente por vez para evitar conflitos.

Cmdlets da ferramenta de configuração automatizada para migração

Esta página lista todos os cmdlets e parâmetros suportados pela ferramenta para casos de uso de migração.

Todos os cmdlets aceitam parâmetros de um dos seguintes tipos.

- String
- Lista de strings
- Booleano: `$true` ou `$false`
- SwitchParameter: a presença do parâmetro significa `$true`; a ausência do parâmetro significa `$false`

> **Nota:**
>
> SwitchParameter é o método preferencial para seleções verdadeiro ou falso, mas booleanos ainda são usados na ferramenta devido a problemas de legado.

> A tabela a seguir é um resumo de todos os cmdlets. Consulte cada seção individual para descobrir quais parâmetros cada cmdlet suporta.

CATEGORIA	CMDLET	DESCRIÇÃO
Migração local para a nuvem	`Export-CvadAcToFile`	Exportar arquivos locais para arquivos YAML.
	`Import-CvadAcToSite`	Importar arquivos YAML para a nuvem. Suporta operações de criação, atualização e exclusão.
	`Merge-CvadAcToSite`	Importar arquivos YAML para a nuvem. Suporta operações de criação e atualização.
	`New-CvadAcToSite`	Importar arquivos YAML para a nuvem. Suporta operações de criação e atualização.
	`Sync-CvadAcToSite`	Exportar e importar em uma única etapa.
	Migração granular Para componentes, use parâmetros com os comandos acima. Exemplos: `MachineCatalogs`, `Tags`. Para nomes de componentes, use parâmetros com os comandos acima. Exemplos: `IncludeByName`, `ExcludeByName`.	Migrar seletivamente apenas componentes ou nomes de componentes
Cmdlets de nuvem para nuvem	`Backup-CvadAcToFile`	Faz backup de toda a configuração do seu site na nuvem.
	`Restore-CvadAcToSite`	Restaura arquivos YAML de backup para o site na nuvem. Este site na nuvem pode ser o mesmo ou diferente do site na nuvem de origem.

CATEGORIA	CMDLET	DESCRIÇÃO
	`Remove-CvadAcFromSite`	Remove membros do componente da nuvem.
	Migração granular Para componentes, use parâmetros com os comandos acima. Exemplos: `MachineCatalogs`, `Tags`. Para nomes de componentes, use parâmetros com os comandos acima. Exemplos: `IncludeByName`, `ExcludeByName`.	Migrar seletivamente apenas componentes ou nomes de componentes
Outros cmdlets básicos	`Compare-CvadAcToSite`	Compara os arquivos .yml locais com a configuração da nuvem.
Cmdlets relacionados a pré-requisitos	`New-CvadAcCustomerInfoFile`	Cria um arquivo de informações do cliente.
	`Set-CvadAcCustomerInfoFile`	Atualiza um arquivo de informações do cliente existente.
Cmdlets de suporte e solução de problemas	`New-CvadAcZipInfoForSupport`	Compacta todos os arquivos de log e .yml em um único arquivo zip para enviar à Citrix® para suporte.
	`Get-CvadAcStatus`	Usado para testar a conectividade e garantir que todos os pré-requisitos sejam atendidos. Retorna informações sobre a ferramenta, como número da versão e conectividade com a nuvem e status do conector.

CATEGORIA	CMDLET	DESCRIÇÃO
	`Test-CvadAcConnectionWithSite`	Testa a conexão com o site da nuvem.
	`Find-CvadAcConnector`	Localiza conectores existentes e determina seu estado de execução.
	`Get-CvadAcCustomerSites`	Retorna a lista de todos os sites do cliente.
	`New-CvadAcTemplateToFile`	Cria um arquivo de modelo para os componentes selecionados.
	`Show-CvadAcDocument`	Exibe esta documentação no navegador padrão.
	`Find-CvadAcInFile`	A pesquisa em arquivo busca em arquivos YAML de componentes por membros que correspondam a um ou mais nomes que podem conter curingas.
Cmdlets de ativação de site	`Set-CvadAcSiteActiveStateOnPrem`	Define o estado do site local como ativo ou inativo.
	`Set-CvadAcSiteActiveStateCloud`	Define o estado do site na nuvem como ativo ou inativo.
Cmdlets de fusão de vários sites locais	`New-CvadAcSiteMergingInfo`	Cria um conjunto de informações de prefixo/sufixo para fusão de sites.
	`Set-CvadAcSiteMergingInfo`	Atualiza um conjunto de informações de prefixo/sufixo de fusão de sites existente.

CATEGORIA	CMDLET	DESCRIÇÃO
	`Remove-CvadAcSiteMergingInfo`	Remove um conjunto de informações de prefixo/sufixo de fusão de site existente.

Para obter mais informações sobre os parâmetros e como usá-los, consulte Parâmetros de migração granular.

Cmdlets básicos

Cmdlets de local para nuvem

- `Export-CvadAcToFile` - Exportar arquivos locais para arquivos YAML.

  Exporta a configuração da sua configuração local. Esta é a operação de exportação padrão para a configuração automatizada. Nenhuma modificação é feita na configuração do site local. Os arquivos exportados são colocados no diretório *%HOMEPATH%\Documents\Citrix\AutoConfig* em uma subpasta **Export** com nome exclusivo. A pasta *%HOMEPATH%\Documents\Citrix\AutoConfig* sempre contém a configuração de site local exportada mais recente.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes		SwitchParameters
Filtragem por nomes de objetos	Consulte Filtragem por nomes de objeto		Lista de strings
`TargetFolder`	Especifica a pasta de destino da exportação.		String
`Locale`	Especifica o idioma do texto legível por humanos que pode ser exportado.		String

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`Quiet`	Suprime o registro em log no console.		SwitchParameter
`AdminAddress`	Especifica o DNS ou endereço IP do Delivery Controller quando a exportação não está sendo executada no Delivery Controller.		String
`CheckUserAndMachines`	Verifica se usuários e máquinas estão no Active Directory. Usuários e máquinas que não estão no Active Directory podem resultar em falhas de importação.		`$true` ou `$false`
`ZipResults`	Compacta os arquivos YAML de backup em um único arquivo zip. O arquivo está na mesma pasta que os arquivos YAML de backup e tem o mesmo nome da pasta.		SwitchParameter

Retorna:

- Consulte Valores de retorno do Cmdlet

Existem três maneiras de importar dados para a nuvem. A execução de cmdlets específicos pode resultar em uma das três combinações de ações no site da nuvem:

- Adicionar, Atualizar e Excluir

- Adicionar e Atualizar apenas
- Adicionar apenas

CMDLET	ADICIONAR	ATUALIZAR	EXCLUIR
Importar	X	X	X
Mesclar	X	X	
Novo	X		

- `Import-CvadAcToSite` - Importar arquivos YAML para a nuvem. Suporta operações de criação, atualização e exclusão.

  Importa todos os arquivos locais para a nuvem. Este comando garante que o estado final da nuvem seja idêntico ao estado local. Esta opção exclui quaisquer alterações existentes na nuvem. Os arquivos de configuração do site importados são originados de *%HOMEPATH%\Documents\Citrix\AutoConfig*. *Use com cautela.*

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes.		SwitchParameters
Filtragem por nomes de objeto	Consulte Filtragem por nomes de objeto.		Lista de strings
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters
`SourceFolder`	Identifica uma pasta raiz substituta para *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Especifica o idioma do texto legível por		String

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	humanos que pode ser exportado.		
`Quiet`	Suprimir o registro no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log ao concluir o cmdlet. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`Merge`	Quando definido como `$true`, apenas adiciona componentes ao site da nuvem. Os componentes não são removidos. Defina como `$false` para remover componentes.		`$true` ou `$false`
`AddOnly`	Quando definido como `$true`, adiciona apenas novos componentes, não atualiza nem exclui componentes existentes. Defina como `$false` para permitir atualizações e exclusões. `Merge` é ignorado quando este parâmetro é `$true`.		`$true` ou `$false`

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`MergePolicies`	Mesclar configurações e filtros de política. A mesclagem ocorre somente quando uma política sendo importada já existe no DDC da nuvem. O resultado da mesclagem de políticas é que as políticas do DDC da nuvem contêm as configurações e filtros que já possuía, além de quaisquer novas configurações e filtros sendo importados. Observe que, quando ocorrem colisões de configurações e filtros, os valores importados têm precedência.		Parâmetro de alternância
`OnErrorAction`	Consulte parâmetro OnErrorAction.		String

Retorna:

- Consulte valores de retorno do Cmdlet

- `Merge-CvadAcToSite` - Importa arquivos YAML para a nuvem. Suporta operações de criação e atualização.

  Mescla os arquivos locais com a nuvem, mas *não* exclui nenhum componente na nuvem ou no site local. Isso preserva as alterações já feitas na nuvem. Se um componente existir no Citrix

Cloud com o mesmo nome, este comando poderá modificar esse componente. Esta é a operação de importação padrão para a configuração automatizada. Os arquivos de configuração do site mesclados são originados de *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes.		SwitchParameters
Filtragem por nomes de objeto	Consulte Filtragem por nomes de objeto.		Lista de strings
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters
`SourceFolder`	Identifica uma pasta raiz substituta para *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Especifica o idioma do texto legível por humanos que pode ser exportado.		String
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log ao concluir o cmdlet. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`Merge`	Quando definido como `$true`,		`$true` ou `$false`

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	adiciona apenas componentes ao site da nuvem. Os componentes não são removidos. Defina como `$false` para remover componentes.		
`AddOnly`	Quando definido como `$true`, adiciona apenas novos componentes, não atualiza nem exclui componentes existentes. Defina como `$false` para permitir atualizações e exclusões. `Merge` é ignorado quando este parâmetro é `$true`.		`$true` ou `$false`
`MergePolicies`	Mesclar configurações e filtros de política. A mesclagem ocorre somente quando uma política que está sendo importada já existe no DDC da nuvem. O resultado da mesclagem de políticas é que as políticas do DDC da nuvem contêm as configurações e os		SwitchParameter

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	filtros que já possuía, além de quaisquer novas configurações e filtros que estão sendo importados. Observe que, quando ocorrem colisões de configurações e filtros, os valores importados têm precedência.		
`OnErrorAction`	Consulte OnErrorAction parâmetro.		String

Retorna:

- Consulte Valores de retorno do cmdlet

- `New-CvadAcToSite` - Importa arquivos YAML para a nuvem. Suporta operações de criação e atualização.

  Importa a configuração do site local para a nuvem, mas apenas adiciona novos componentes. Os componentes existentes do site na nuvem não são atualizados nem excluídos. Use este comando se os componentes existentes do seu site na nuvem devem permanecer inalterados.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes.		SwitchParameters
Filtragem por nomes de objeto	Consulte Filtragem por nomes de objeto.		Lista de strings

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters
`SourceFolder`	Identifica uma pasta raiz substituta para *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Especifica o idioma do texto legível por humanos que pode ser exportado.		String
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log ao concluir o cmdlet. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`OnErrorAction`	Consulte OnErrorAction parameter.		String

Retorna:

- Consulte Cmdlet return values

- `Sync-CvadAcToSite` - Exportar e importar em uma única etapa.

  A sincronização executa tanto uma exportação quanto uma importação em uma única etapa. Use o parâmetro `SourceTargetFolder` para especificar a pasta de destino de exportação/importação.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrate by components		SwitchParameters
Filtragem por nomes de objeto	Consulte Filtragem por nomes de objeto		Lista de strings
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`SourceTargetFolder`	Especifica a pasta de destino de exportação/ importação.		String
`Locale`	Especifica o idioma do texto legível por humanos que pode ser exportado.		String
`AdminAddress`	Especifica o DNS ou endereço IP do controlador de entrega quando a exportação não está sendo executada no controlador de entrega.		String
`Quiet`	Suprime o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log ao concluir o cmdlet. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`Merge`	Quando definido como `$true`, apenas adiciona componentes ao site da nuvem. Os componentes não são removidos. Defina como `$false` para remover componentes.		`$true` ou `$false`
`AddOnly`	Quando definido como `$true`, adiciona apenas novos componentes, não atualiza nem exclui componentes existentes. Defina como `$false` para permitir atualizações e exclusões. `Merge` é ignorado quando este parâmetro é `$true`.		`$true` ou `$false`
`MergePolicies`	Mesclar configurações e filtros de política. A mesclagem ocorre somente quando uma política que está sendo importada já existe no DDC da nuvem. O resultado da mesclagem de políticas é que as políticas do DDC da		SwitchParameter

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	nuvem contêm as configurações e os filtros que já possuía, além de quaisquer novas configurações e filtros que estão sendo importados. Observe que, quando ocorrem colisões de configurações e filtros, os valores importados têm precedência.		

Retorna:

- Consulte Valores de retorno do Cmdlet

Cmdlets de nuvem para nuvem

- `Backup-CvadAcToFile` - Faz backup de toda a configuração do seu site na nuvem.

  Exporta sua configuração de nuvem para arquivos .yml. Este backup pode ser usado em um processo de backup e restauração para restaurar componentes perdidos.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes		SwitchParameters
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`TargetFolder`	Especifica a pasta de destino da exportação.		String

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`Locale`	Especifica o idioma do texto legível por humanos que pode ser exportado.		String
`Quiet`	Suprime o registro em log para o console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log na conclusão do cmdlet. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`ZipResults`	Compacta arquivos YAML de backup em um único arquivo zip. O arquivo está na mesma pasta que os arquivos YAML de backup e tem o mesmo nome da pasta.		SwitchParameter

Retorna:

- Consulte Valores de retorno do Cmdlet

- `Restore-CvadAcToSite` - Restaura arquivos YAML de backup para o site da nuvem. Este site da nuvem pode ser o mesmo ou diferente do site da nuvem de origem.

  Restaura o site da nuvem para a configuração anterior. Os arquivos importados são originados da pasta especificada usando o parâmetro `-RestoreFolder`, que identifica a pasta contendo os arquivos .yml a serem restaurados para o site da nuvem. Esta deve ser uma especificação de pasta totalmente qualificada. Este cmdlet pode ser usado para reverter para sua configuração anterior ou para fazer backup e restaurar seu site da nuvem. Este comando pode adicionar, excluir e atualizar seu site da nuvem.

Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes.		SwitchParameters
Filtragem por nomes de objeto	Consulte Filtragem por nomes de objeto.		Lista de strings
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters
`RestoreFolder`	Identifica a pasta que contém os arquivos .yml a serem restaurados para o site da nuvem. Esta deve ser uma especificação de pasta totalmente qualificada.		String
`Locale`	Especifica o idioma do texto legível por humanos que pode ser exportado.		String
`Quiet`	Suprime o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log ao concluir o cmdlet. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`Merge`	Quando definido como `$true`,		`$true` ou `$false`

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	adiciona apenas componentes ao site da nuvem. Os componentes não são removidos. Defina como `$false` para remover componentes.		
`AddOnly`	Quando definido como `$true`, adiciona apenas novos componentes, não atualiza nem exclui componentes existentes. Defina como `$false` para permitir atualizações e exclusões. `Merge` é ignorado quando este parâmetro é `$true`.		`$true` ou `$false`
`MergePolicies`	Mesclar configurações e filtros de política. A mesclagem ocorre somente quando uma política sendo importada já existe no DDC da nuvem. O resultado da mesclagem de políticas é que as políticas do DDC da nuvem contêm as configurações e os filtros que já		SwitchParameter

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	possuía, além de quaisquer novas configurações e filtros que estão sendo importados. Observe que, quando ocorrem colisões de configurações e filtros, os valores importados têm precedência.		
`OnErrorAction`	Consulte parâmetro OnErrorAction.		String

Retorna:

- Consulte Valores de retorno do Cmdlet

- `Remove-CvadAcFromSite` – Remove membros do componente da nuvem.

  Pode redefinir o site inteiro ou remover itens de membro de um componente (Por exemplo, remover um catálogo de máquinas da lista de catálogos). Isso pode ser usado quando acoplado ao parâmetro `IncludeByName` para remover seletivamente membros específicos.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes		SwitchParameters
Filtragem por nomes de objeto	Consulte Filtragem por nomes de objeto		Lista de strings
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`Quiet`	Suprime o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log ao concluir o cmdlet. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`

Retorna:

- Consulte Valores de retorno do cmdlet

Outros cmdlets básicos

- `Compare-CvadAcToSite` - Compara os arquivos .yml locais com a configuração da nuvem, produzindo um relatório de alterações feitas por um cmdlet `Import`, `Merge` ou `Restore`.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes.		SwitchParameters
Filtragem por nomes de objeto	Consulte Filtragem por nomes de objeto.		Lista de strings
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters
`SourceFolder`	Identifica uma pasta raiz substituta para *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`Locale`	Especifica o idioma do texto legível por humanos que pode ser exportado.		String
`Quiet`	Suprime o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log na conclusão do cmdlet. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`Merge`	Quando definido como `$true`, apenas adiciona componentes ao site da nuvem. Os componentes não são removidos. Defina como `$false` para remover componentes.		`$true` ou `$false`
`AddOnly`	Quando definido como `$true`, adiciona apenas novos componentes, não atualiza nem exclui componentes existentes. Defina como `$false` para permitir atualizações e exclusões. `Merge` é ignorado quando		`$true` ou `$false`

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	este parâmetro é `$true`.		
`OnErrorAction`	Consulte OnErrorAction parameter.		String

Retorna:

- Consulte Cmdlet return values

Parâmetros de migração granular

Migrar por componentes

Os seguintes componentes podem ser especificados com cmdlets que os suportam. A opção `All` é selecionada automaticamente quando nenhum parâmetro de componente é especificado. Para evitar erros, recomendamos que você migre os componentes na seguinte ordem:

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

Filtragem por nomes de objeto

Migrar por nomes de componente

Os parâmetros `IncludeByName` e `ExcludeByName` permitem incluir e excluir membros de componentes em cmdlets por nome. Apenas um componente (por exemplo, grupos de entrega) pode ser escolhido por vez em qualquer um dos cmdlets suportados. Se um membro do componente estiver em ambas as áreas, a exclusão substitui qualquer outro parâmetro e uma entrada é feita na lista de correção de log identificando o componente e o nome do membro que foi excluído.

`IncludeByName` e `ExcludeByName` aceitam uma lista de nomes de membros de componentes. Qualquer nome pode conter um ou mais curingas. Dois tipos de curingas são suportados. A lista de nomes de membros de componentes deve ser colocada entre aspas simples quando qualquer nome de membro contiver caracteres especiais.

- * Corresponde a qualquer número de caracteres
- ? Corresponde a um único caractere

`IncludeByName` e `ExcludeByName` também podem aceitar um arquivo contendo uma lista de membros, onde cada membro pode ser explícito ou conter curingas. Cada linha no arquivo pode conter um membro. Espaços iniciais e finais são removidos do nome do membro. O nome do arquivo deve ser precedido pelo sinal @ e estar entre aspas simples (um requisito do PowerShell para que o @ não seja reinterpretado). Vários arquivos podem ser listados, além de serem misturados com nomes de membros.

Um exemplo de mesclagem de todos os grupos de entrega cujos nomes começam com `DgSite1` e contêm `Home2` seria escrito:

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

Por Nome do Grupo de Entrega

`ByDeliveryGroupName` filtra pelo nome do grupo de entrega para aplicativos e grupos de aplicativos. Este parâmetro é sempre uma lista de inclusão que identifica os membros a serem incluídos com base em sua associação ao grupo de entrega.

`ByDeliveryGroupName` aceita uma lista de nomes de grupos de entrega. Qualquer nome pode conter um ou mais curingas. Dois tipos de curingas são suportados.

- * corresponde a qualquer número de caracteres
- ? corresponde a um único caractere

O exemplo a seguir mescla todos os aplicativos que fazem referência a todos os nomes de grupos de entrega que começam com `EastDg`.

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

Excluir Desabilitados

`ExcludeDisabled` filtra das operações de importação todos os aplicativos e grupos de aplicativos que estão desabilitados. `ExcludeDisabled` assume o valor padrão `false`, o que significa que todos os aplicativos e grupos de aplicativos são importados independentemente do seu estado habilitado.

Por Nome da Máquina

`ByMachineName` filtra pelo nome da máquina para catálogos de máquinas e grupos de entrega. Este parâmetro é sempre uma lista de inclusão que identifica os membros a serem incluídos com base em sua associação ao nome da máquina.

`ByMachineName` aceita uma lista de nomes de máquinas onde qualquer nome pode conter um ou mais curingas. Dois tipos de curingas são suportados.

- * corresponde a qualquer número de caracteres
- ? corresponde a um único caractere

Ao exportar ou importar e usar `ByMachineName`, se um filtro de nome de máquina resultar em nenhuma máquina no catálogo de máquinas ou grupo de entrega, o catálogo de máquinas ou grupo de entrega será excluído da exportação ou importação.

> **Nota:**
>
> O uso de `ByMachineName` em qualquer cmdlet de tipo de importação resulta em `MergeMachines` sendo definido como `$true`.

Mesclar Máquinas

`MergeMachines`, quando definido como `$true`, instrui a operação de importação a adicionar máquinas apenas ao catálogo de máquinas ou grupo de entrega. As máquinas não são removidas, permitindo operações aditivas incrementais.

`MergeMachines` assume o valor padrão false, o que significa que as máquinas são removidas se não estiverem presentes no arquivo .yml do catálogo de máquinas ou grupo de entrega.

`MergeMachines` é definido como `$true` quando `ByMachineName` é usado, mas pode ser substituído definindo `MergeMachines` como false.

Cmdlets relacionados a pré-requisitos

- `New-CvadAcCustomerInfoFile` - Crie um arquivo de informações do cliente. Por padrão, o arquivo de informações do cliente está localizado em *%HOMEPATH%\Documents\Citrix\AutoConfig*.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`CustomerId`	ID do cliente.	x	String
`ClientId`	ID de cliente do cliente criado no Citrix Cloud. O CustomerId e o Secret devem ser especificados ao usar este parâmetro.	Condicionalmente	String
`Secret`	Chave secreta do cliente criada no Citrix Cloud. O CustomerId e o ClientId devem ser especificados ao usar este parâmetro.	Condicionalmente	String
`Environment`	Ambiente Production, ProductionGov ou ProductionJP.		Enumeração
`LogFileName`	Altere o prefixo do arquivo de log de CitrixLog para outra coisa.		String

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`AltRootUrl`	Usar somente sob a direção da Citrix.		String
`StopOnError`	Interrompe a operação no primeiro erro.		`$true` ou `$false`
`TargetFolder`	Use a pasta especificada como pasta raiz em vez de *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Use o local especificado em vez do local derivado do sistema em que a ferramenta é executada.		String
`Editor`	Use o editor especificado para exibir o log ao concluir cada cmdlet. Notepad.exe é o editor padrão. Este parâmetro deve incluir a especificação de arquivo totalmente qualificada para o editor e o editor deve usar a especificação do arquivo de log como seu único parâmetro.		String

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`SecurityCsvFileSpec`	A especificação de arquivo totalmente qualificada apontando para o arquivo SecurityClient.csv baixado do Citrix Identity and Access Management. O CustomerId deve ser especificado ao usar este parâmetro.		String

Retorna:

- Consulte Valores de retorno do Cmdlet

- `Set-CvadAcCustomerInfoFile` - Atualiza um arquivo de informações do cliente existente. Apenas os parâmetros especificados do cmdlet são alterados. Todos os valores de parâmetros não especificados no arquivo CustomerInfo.yml permanecem inalterados.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`CustomerId`	ID do cliente.		String
`ClientId`	ID do cliente do cliente criada no Citrix Cloud.		String
`Secret`	Chave secreta do cliente criada no Citrix Cloud.		String
`Environment`	Ambiente de Produção, ProductionGov ou ProductionJP.		Enumeração

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`LogFileName`	Altera o prefixo do arquivo de log de CitrixLog para outro.		String
`StopOnError`	Interrompe a operação no primeiro erro.		`$true` ou `$false`
`TargetFolder`	Use a pasta especificada como pasta raiz em vez de *%HOMEPATH%\Documents\Citrix\AutoConfig*.		String
`Locale`	Use o local especificado em vez do local derivado do sistema em que a ferramenta é executada.		String
`Editor`	Use o editor especificado para exibir o log na conclusão de cada cmdlet. Notepad.exe é o editor padrão. Este parâmetro deve incluir a especificação de arquivo totalmente qualificada para o editor, e o editor deve aceitar a especificação do arquivo de log como		String

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	seu único parâmetro.		
`SecurityCsvFileSpec`	A especificação de arquivo totalmente qualificada apontando para o arquivo SecurityClient.csv baixado do Citrix Identity and Access Management. O CustomerId deve ser especificado ao usar este parâmetro.		String

Retorna:

- Consulte Valores de retorno do cmdlet

Parâmetros relacionados aos pré-requisitos

Juntamente com os parâmetros de acesso à nuvem, os seguintes parâmetros podem ser usados com os cmdlets relacionados aos pré-requisitos:

- `Environment` – Ambiente de Produção ou ProductionGov.
- `LogFileName` – Mudar o prefixo do arquivo de log de CitrixLog para outra coisa.
- `StopOnError` – Interrompe a operação no primeiro erro.
- `AlternateRootFolder` – Usar a pasta especificada como pasta raiz em vez de *%HOMEPATH%\Documents\Citrix\AutoConfig*.
- `Locale` – usar o local especificado em vez do local derivado do sistema em que a ferramenta é executada.
- `Editor` – usar o editor especificado para exibir o log na conclusão de cada cmdlet. Notepad.exe é o editor padrão. Este parâmetro deve incluir a especificação de arquivo totalmente qualificada para o editor e o editor deve aceitar a especificação do arquivo de log como seu único parâmetro.

Cmdlets de suporte e solução de problemas

- `New-CvadAcZipInfoForSupport` - Compacta todos os arquivos de log e .yml em um único arquivo zip para enviar à Citrix para suporte. Informações confidenciais do cliente (CustomerInfo.yml e CvadAcSecurity.yml) não são incluídas no zip. O arquivo Icon.yml também é excluído devido ao seu tamanho. O arquivo zip é colocado em *%HOMEPATH%\Documents\Citrix\AutoConfig* e nomeado *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, com base na data e hora. Este arquivo zip também pode atuar como um backup.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`TargetFolder`	Especifica uma pasta de destino para criar e salvar o arquivo zip.		String
`Quiet`	Suprime o registro no console.		SwitchParameter

  Retorna:

  - O arquivo zip com o nome e o local do arquivo zip é exibido no prompt de comando.

- `Get-CvadAcStatus` - Use para testar a conectividade e garantir que todos os pré-requisitos sejam atendidos. Retorna informações sobre a ferramenta, como número da versão e conectividade com a nuvem e status do conector.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`SiteId`	Identifica o site ao qual se conectar.		String
`AdminAddress`	Este é o endereço DNS ou IP do Delivery Controller		String

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	local usado para verificar o nível de acesso dos administradores. Isso é necessário se a ferramenta não estiver sendo executada em um Delivery Controller.		

Retorna:

- Exibe os resultados para cada item.

- `Test-CvadAcConnectionWithSite` – Teste a conexão com o site da nuvem para verificar se a conexão de comunicação está funcionando. Este cmdlet usa os parâmetros de acesso à nuvem ou o arquivo CustomerInfo.yml para especificar as informações de conexão do cliente.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`Quiet`	Suprimir o registro no console.		SwitchParameter

  Retorna:

  - Os resultados do teste são exibidos na linha de comando.

- `Find-CvadAcConnector` - Localiza conectores existentes e determina seu estado de execução. Este cmdlet usa informações do arquivo CustomerInfo.yml ou do parâmetro de ID do cliente para localizar os conectores do cliente.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`CustomerInfoFileSpec`	A especificação do arquivo apontando para um arquivo de informações do cliente para substituir o local e o nome padrão. Este parâmetro é ignorado quando o parâmetro `CustomerId` é fornecido.		String
`CustomerId`	O ID do cliente. Este parâmetro substitui o mesmo valor no arquivo CustomerInfo.yml.		String

Retorna:

- Os resultados são exibidos na linha de comando.

- `Get-CvadAcCustomerSites` - Retorna a lista de todos os sites do cliente. Este cmdlet usa os parâmetros de acesso à nuvem ou o arquivo CustomerInfo.yml para especificar as informações de conexão do cliente.

  Parâmetros:

  - Consulte Parâmetros de acesso à nuvem

  Retorna:

  - Exibe uma lista de IDs de sites de clientes encontrados.

- `New-CvadAcTemplateToFile` – Cria um arquivo de modelo para os componentes selecionados, permitindo que você crie manualmente um arquivo de importação.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes		SwitchParameters
`TargetFolder`	Especifica a pasta de destino da exportação.		String

Retorna:

- Consulte Valores de retorno do Cmdlet

- `Show-CvadAcDocument` - Exibe esta documentação no navegador padrão.

  Parâmetros:

  - Nenhum.

  Retorna:

  - Exibe esta página da web no navegador padrão.

- `Find-CvadAcInFile` - A pesquisa em arquivo procura em arquivos YAML de componentes por membros que correspondam a um ou mais nomes que podem conter curingas. O resultado é um relatório de membros encontrados. A pesquisa em arquivo pode pesquisar apenas um componente por vez. A pesquisa em arquivo procura em todos os arquivos YAML na pasta atual e em todas as subpastas. Use `FindSourceFolder` para limitar o número de arquivos a serem pesquisados.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes. Observação: O valor `-All` não é válido.		SwitchParameters
`IncludeByName`	Uma lista especificando os nomes dos grupos		Lista de strings

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	de entrega a serem incluídos ao definir o estado ativo do site como ativo. Os curingas '*' e '?' são suportados nos nomes.		
`Unique`	Relatar apenas membros encontrados exclusivos.		SwitchParameter
`IncludeYaml`	Incluir o YAML específico do membro.		SwitchParameter
`FindSourceFolder`	A pasta em que a pesquisa começa.		String
`DisplayLog`	Exibe o arquivo de log ao concluir o cmdlet. Defina como `$false` para suprimir a exibição do log.		SwitchParameter
`Quiet`	Suprimir o registro em log no console.		SwitchParameter

Retorno:

- Cria um relatório contendo os membros encontrados para o componente especificado.

Cmdlets de ativação de site

Para obter mais informações sobre como ativar sites e o uso desses cmdlets, consulte Ativando sites.

- `Set-CvadAcSiteActiveStateOnPrem` - Define o estado do site local como ativo ou inativo.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`SiteActive`	Quando presente, define o site local como ativo, removendo o modo de manutenção de todos os grupos de entrega. Quando este parâmetro não está presente, o modo de manutenção é definido em todos os grupos de entrega.		SwitchParameter
`IncludeByName`	Uma lista que especifica os nomes dos grupos de entrega a serem incluídos ao definir o estado ativo do site como ativo. Os curingas ‘*’ e ‘?’ são suportados nos nomes.		Lista de strings
`ExcludeByName`	Uma lista especificando os nomes dos grupos de entrega a serem excluídos ao definir o estado ativo do site como ativo. Os curingas '*' e '?' são suportados nos nomes.		Lista de strings

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log ao concluir o cmdlet. Defina como `$false` para suprimir a exibição do log.		`$true or $false`

Retorna:

- Consulte Valores de retorno do Cmdlet

- `Set-CvadAcSiteActiveStateCloud` - Define o estado do site na nuvem como ativo ou inativo.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`SiteActive`	Quando presente, define o site da nuvem como ativo, removendo o modo de manutenção de todos os grupos de entrega. Quando este parâmetro não está presente, o modo de manutenção é definido em todos os grupos de entrega.		SwitchParameter

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`IncludeByName`	Uma lista especificando os nomes dos grupos de entrega a serem incluídos ao definir o estado ativo do site como ativo. Os curingas '*' e '?' são suportados nos nomes.		Lista de strings
`ExcludeByName`	Uma lista especificando os nomes dos grupos de entrega a serem excluídos ao definir o estado ativo do site como ativo. Os curingas '*' e '?' são suportados nos nomes.		Lista de strings
`Quiet`	Suprimir o registro no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log ao concluir o cmdlet. Defina como `$false` para suprimir a exibição do log.		`$true or $false`

Retorna:

- Consulte Valores de retorno do cmdlet

Cmdlets para mesclar vários sites locais

Para obter mais informações sobre a mesclagem de sites e o uso desses cmdlets, consulte Mesclar vários sites em um único site.

- `New-CvadAcSiteMergingInfo` - Cria um conjunto de informações de prefixo/sufixo de mesclagem de sites. Não é necessário saber todos os prefixos ou sufixos no início. Eles podem ser atualizados com `Set-CvadAcSiteMergingInfo` ou editando manualmente o arquivo SiteMerging.yml. Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`SiteName`	O nome usado para identificar o conjunto de prefixos/sufixos para um site específico. Pode corresponder ao nome do site real, mas não é obrigatório.	x	String
Parâmetros de mesclagem de sites	Consulte Parâmetros de mesclagem de sites		SwitchParameters
`Quiet`	Suprimir o registro no console.		SwitchParameter

  Retorna:

  - Nenhum

- `Set-CvadAcSiteMergingInfo` - Atualiza um conjunto de informações de prefixo/sufixo de mesclagem de site existente.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`SiteName`	O nome usado para identificar o conjunto de prefixos/sufixos para um site específico. Pode corresponder ao	x	String

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	nome do site real, mas não é obrigatório.		
Parâmetros de mesclagem de sites	Consulte Parâmetros de mesclagem de sites		SwitchParameters
`Quiet`	Suprimir o registro em log no console.		SwitchParameter

Retorna:

- Nenhum

- `Remove-CvadAcSiteMergingInfo` - Remove um conjunto de informações de prefixo/sufixo de mesclagem de site existente.

  Parâmetros:

  - `SiteName` – identifica o conjunto de prefixos e sufixos do site. É uma string e é obrigatório.

  Retorna:

  - Nenhum

Parâmetros de mesclagem de sites

Os seguintes parâmetros podem ser usados ao executar os cmdlets de mesclagem de sites. Todos os parâmetros listados são strings.

- `SiteName` – o nome usado para identificar o conjunto de prefixos/sufixos para um site específico. Pode corresponder ao nome do site real, mas não é necessário. SiteName é um parâmetro obrigatório.
- `AdminScopedPrefix` – o prefixo a ser aplicado aos escopos do administrador.
- `ApplicationPrefix` - o prefixo a ser aplicado aos aplicativos.
- `ApplicationFolderPrefix` – o prefixo a ser aplicado às pastas de aplicativos; `ApplicationFolderPrefix` pode ser combinado com `ApplicationFolderRoot`.

- `ApplicationFolderRoot` – a nova pasta raiz para pastas de aplicativos. Isso cria uma hierarquia de pastas extra. `ApplicationFolderRoot` pode ser combinado com `ApplicationFolderPrefix`.
- `ApplicationGroupPrefix` – o prefixo para grupos de aplicativos.
- `ApplicationUserPrefix` – o prefixo a ser aplicado ao nome do aplicativo que o usuário vê.
- `ApplicationAdminPrefix` – o prefixo a ser aplicado ao nome do aplicativo que o administrador vê.
- `DeliveryGroupPrefix` – o prefixo a ser aplicado aos grupos de entrega.
- `GroupPolicyPrefix` – o prefixo a ser aplicado a nomes de políticas.
- `HostConnectionPrefix` – o prefixo a ser aplicado a conexões de host.
- `MachineCatalogPrefix` – o prefixo a ser aplicado a catálogos de máquinas.
- `StoreFrontPrefix` – o prefixo a ser aplicado a nomes do StoreFront™.
- `TagPrefix` – o prefixo a ser aplicado a tags.
- `AdminScopedSuffix` – o sufixo a ser aplicado a escopos de administrador.
- `ApplicationSuffix` - o sufixo a ser aplicado a aplicativos.
- `ApplicationFolderSuffix` – o sufixo a ser aplicado a pastas de aplicativos; `ApplicationFolderSuffix` pode ser combinado com `ApplicationFolderRoot`.
- `ApplicationGroupSuffix` – o sufixo para grupos de aplicativos.
- `ApplicationUserSuffix` – o sufixo a ser aplicado ao nome do aplicativo que o usuário vê.
- `ApplicationAdminSuffix` – o sufixo a ser aplicado ao nome do aplicativo que o administrador vê.
- `DeliveryGroupSuffix` – o sufixo a ser aplicado a grupos de entrega.
- `GroupPolicySuffix` – o sufixo a ser aplicado a nomes de políticas.
- `HostConnectionSuffix` – o sufixo a ser aplicado a conexões de host.
- `MachineCatalogSuffix` – o sufixo a ser aplicado a catálogos de máquinas.
- `StoreFrontSuffix` – o sufixo a ser aplicado aos nomes do StoreFront.
- `TagSuffix` – o sufixo a ser aplicado às tags.
- `SiteRootFolder` – o nome de pasta totalmente qualificado a ser usado para exportações e importações; pode ser uma pasta local ou um compartilhamento de arquivos.

Parâmetros genéricos

Parâmetros de acesso à nuvem

Todos os cmdlets que acessam a nuvem suportam os seguintes parâmetros extras.

> **Nota:**
>
> O CustomerId, ClientId e Secret podem ser colocados no arquivo CustomerInfo.yml ou especificados com o cmdlet usando os seguintes parâmetros. Quando são especificados em ambos os locais, os parâmetros do cmdlet têm precedência.

- `CustomerId` – O ID do cliente usado nas APIs Rest e é necessário para acessar todas as APIs Rest. Seu ID de cliente é encontrado no Citrix Cloud.
- `ClientId` – O clientID criado no site de Gerenciamento de Identidade e Acesso do Citrix Cloud. Isso é necessário para obter o token de portador necessário para autenticação para todas as APIs Rest.
- `Secret` – A chave secreta criada no site de Gerenciamento de Identidade e Acesso do Citrix Cloud. Isso é necessário para obter o token de portador necessário para autenticação para todas as APIs Rest.
- `CustomerInfoFileSpec` – A especificação do arquivo apontando para um arquivo de informações do cliente para substituir o local e o nome padrão.

Parâmetros do modo de migração

Os cmdlets que modificam a configuração do site na nuvem (`Import`, `Restore`, `Merge`, `New` e `Sync`) suportam os seguintes parâmetros extras para fornecer maior flexibilidade.

- `CheckMode` – Executa a operação de importação, mas *não* faz alterações. Todas as alterações esperadas são relatadas antes da conclusão da importação. Você pode usar este comando para testar sua importação antes que ela ocorra.
- `BackupFirst` – Faz backup do conteúdo da nuvem para arquivos .yml antes de modificar a configuração da nuvem. Isso é habilitado por padrão.
- `Confirm` – Quando verdadeiro, solicita aos usuários que confirmem se desejam fazer alterações na configuração do site na nuvem. O cmdlet `Remove` exibe um prompt devido à sua natureza destrutiva. Defina como falso se nenhum prompt for desejado, como ao executar dentro de scripts automatizados. `Confirm` assume o valor verdadeiro por padrão.

- `SecurityFileFolder` – Esta é a pasta totalmente qualificada que contém o arquivo CustomerInfo.yml, que pode apontar para uma pasta local ou uma pasta de compartilhamento de rede que pode estar sob controle de autenticação. A ferramenta não solicitará credenciais; o acesso ao recurso controlado deve ser obtido antes de executar a ferramenta.
- `SiteName` – Especifica o conjunto de prefixo e sufixo de mesclagem do site a ser usado na importação.
- `SiteActive` – Especifica se o site importado está ativo ou inativo. Por padrão, este parâmetro é definido como `$false`, o que significa que o site importado está inativo.

Parâmetros de exibição de log

Os cmdlets `Export`, `Import`, `Sync`, `Restore`, `Backup`, `Compare` e `Remove` exibem o arquivo de log quando a operação é concluída. Você pode suprimir a exibição definindo o parâmetro `-DisplayLog` como `$false`. O Notepad.exe é usado por padrão para exibir o arquivo de log. Você pode especificar um editor diferente no arquivo CustomerInfo.yml.

`Editor: C:\Program Files\Notepad++\notepad++.exe`

Valores de retorno do cmdlet

ActionResult

Todos os cmdlets retornam o seguinte valor.

```
public class ActionResult

{

    public bool                         Overall_Success;

    public Dictionary&lt;string, string>   Individual_Success;

    public object                       CustomResult;

}
```

`Overall_Success` retorna um único booleano mostrando o sucesso geral do cmdlet em todos os componentes selecionados: verdadeiro significa bem-sucedido e falso significa malsucedido.

`Individual_Success` retorna um ou três valores para cada componente principal. O resultado de um componente pode ser Sucesso, Falha ou Ignorado. Ignorado indica que o componente não foi selecionado para execução pelo cmdlet.

`CustomResult` é específico do cmdlet.

CustomResult

`Import`, `Merge`, `Restore`, `Sync`, `Compare`, `Compare File` e `Remove` retornam as seguintes informações de resultado personalizadas para uma única instância de `EvaluationResultData`.

> **Observação:**
>
> `Export` e `Template` cmdlets não retornam um resultado personalizado.

```
 public class EvaluationResultData

 {

     public Dictionary<string, Dictionary&lt;string, ActionResultValues >>
EvaluationResults;

     public int                  Added;

     public int                  Updated;

     public int                  Deleted;

     public int                  NoChange;

     public int                  TotalChanged;

     public EvaluationResults     OverallResult;

     public string               CloudBackupFolder;

     public string               SourceBackupFolder;

 }
```

```
 Where:

 public enum ActionResultValues

{

     Add,

     Update,

     Delete,

     Identical,

     DoNothing

 }

 public enum EvaluationResults

 {

     Success,

     Failure,

     Skipped

 }
```

`EvaluationResults` exibe uma lista com uma entrada por componente selecionado. A chave é o nome do componente e o valor é uma lista de cada membro do componente e a ação realizada nesse membro do componente. As ações podem ser qualquer um dos valores `ActionResultValues`.

`Added`, `Updated`, `Deleted` e `NoChange` indicam o número total de membros do componente adicionados, atualizados, excluídos ou nenhuma ação realizada, nessa ordem.

`TotalChanged` é a soma de `Added`, `Updated` e `Deleted`.

`OverallResult` é um único booleano que indica o resultado do cmdlet. Verdadeiro indica sucesso total em todos os componentes e falso indica falha no processamento de um ou mais componentes.

`CloudBackupFolder` é a especificação de arquivo totalmente qualificada do backup da configuração do site na nuvem antes que o cmdlet execute quaisquer ações de modificação na nuvem.

`SourceBackupFolder` é a especificação de arquivo totalmente qualificada do backup do arquivo de origem feito após a conclusão do cmdlet. Por padrão, esses arquivos estão em *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Ajuda do PowerShell

A ajuda do PowerShell está disponível para cada cmdlet. Todos os parâmetros são documentados com cada cmdlet, juntamente com uma breve explicação do cmdlet. Para acessar a ajuda de qualquer cmdlet, digite `Get-Help` na frente do cmdlet.

```
Get-Help Import-CvadAcToSite
```

Cmdlets da ferramenta de configuração automatizada para backup e restauração

Esta página lista todos os cmdlets e parâmetros suportados pela ferramenta para acionar as APIs de backup e restauração que o Studio utiliza.

Cmdlets de armazenamento de backup

Get-BckRstrStorage

Este cmdlet é aplicável apenas a ambientes locais. Obtém detalhes para o armazenamento onde os backups são salvos.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.

PARÂMETRO	DESCRIÇÃO
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.

Set-BckRstrStorage

Este cmdlet é aplicável apenas a ambientes locais. Define um novo armazenamento onde os backups são salvos.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.

PARÂMETRO	DESCRIÇÃO
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`MaximumBackups`	O número máximo de backups não fixados a serem persistidos até que o processo de limpeza de backup remova os backups mais antigos quando novos backups forem criados.
`MaximumPinnedBackups`	O número máximo de backups fixados a serem persistidos. Esses backups não são removidos pelo processo de limpeza.
`BlobStorageType`	O tipo de armazenamento: `FileStorage` ou `CustomerAzureStorage`.

PARÂMETRO	DESCRIÇÃO
`FileStoragefolder`	A especificação de pasta totalmente qualificada para a opção `BlobStorageType` `FileStorage`.
`Info1`	Para `FileStorage`, `UserName` opcional Para `CustomerAzureStorage`, o URL SAS do Azure
`Info2`	Para `FileStorage`, Senha opcional
`Info3` e `Info4`	Não utilizado

Test-BckRstrStorage

Este cmdlet é aplicável apenas a ambientes locais. Testa para determinar se o armazenamento definido é válido.

Para `FileStorage`, o teste verifica se a pasta existe e pode ser gravada.

Para `CustomerAzureStorage`, o teste verifica se a URL SAS tem as permissões corretas e se a data atual está entre a data de início e a data de término da URL.

Retorna `true` se for válido e `false` se for inválido.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.

PARÂMETRO	DESCRIÇÃO
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.

Cmdlets de backup

Get-BckRstrBackups

Enumera backups armazenados no local de armazenamento de blob de Backup ou Restauração. Para Citrix Virtual Apps and Desktops™, este local é configurado pelo administrador através do WebStudio. Para DaaS, este é o armazenamento Azure pré-existente do cliente. Use `Get-BckRstrBackupsWithDetiails` para obter informações completas sobre cada backup. Os detalhes do backup incluem o seguinte:

- Nome do Backup
- Notas
- Fixado (verdadeiro ou falso)
- Data e hora do backup
- UID do Histórico
- UID Relacionado (UID do último registro de histórico de Restauração)
- Data e hora relacionadas
- Relacionado se executado em modo de verificação
- Duração em segundos

- Nome do administrador
- Detalhes que enumeram cada componente e a contagem de membros em cada componente.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.

Get-BckRstrBackupsMembers

Enumera os membros de um único componente armazenados em um backup selecionado. Os nomes dos membros são retornados em uma lista simples.

Os componentes são:

- Tags
- AdminScopes

- AdminRoles
- AdminAdministrators (somente local)
- HostConnections
- Ícones
- AdminFolders
- Catálogos de Máquinas
- StoreFronts
- Grupos de Entrega
- Grupos de Aplicativos
- Pastas de Aplicativos
- Aplicativos
- Servidores AppV
- Descoberta de Pacotes AppLib
- Grupos de Isolamento AppV
- Diretivas de Grupo
- Preferências de Zona do Usuário
- Dados do Site
- Zonas (somente no local)

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do

PARÂMETRO	DESCRIÇÃO
	cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: SDK Remoto do PowerShell v2 para Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`BackupName`	O nome do backup. A extensão `.zip` é opcional.
`Component`	Os componentes a serem incluídos no backup.

New-BckRstrBackup

Inicia uma nova ação de backup no Delivery Controller. Esta ação é assíncrona ao cmdlet `New-BckRstrBackup`.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do

PARÂMETRO	DESCRIÇÃO
	cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`Notes`	As notas sobre o backup.
`PollForCompletion`	O parâmetro para sondar a ação em execução no Delivery Controller até que a ação seja concluída. A sondagem registra o progresso e os resultados da conclusão no console, a menos que o parâmetro `Quite` seja especificado.

Cmdlets de fixação de backups

Set-BckRstrPinBackups

Fixa um backup para que ele não seja removido como parte do processo de limpeza de backup do Delivery Controller.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.

PARÂMETRO	DESCRIÇÃO
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`BackupName`	O nome do backup. A extensão `.zip` é opcional.

Set-BckRstrUnpinBackups

Desafixa um backup para que ele esteja disponível para ser removido no processo de limpeza de backup do Delivery Controller.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.

PARÂMETRO	DESCRIÇÃO
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`BackupName`	O nome do backup. A extensão `.zip` é opcional.

Remover cmdlet de backup

Remove-BckRstrBackup

Remove um ou mais backups.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.

PARÂMETRO	DESCRIÇÃO
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`IncludeByName`	O filtro para especificar quais membros do componente considerar para restauração. Esta é uma lista de valores de filtro separados por vírgulas e pode conter os caracteres curinga `*` e `?`.

Cmdlets de backups agendados

Get-BckRstrSchedules

Obtém uma lista de agendamentos de backup.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.

PARÂMETRO	DESCRIÇÃO
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`BackupName`	O nome do backup. A extensão `.zip` é opcional.
`Notes`	As notas a serem definidas ou alteradas.

New-BckRstrSchedule

Cria um novo agendamento de backup.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.

PARÂMETRO	DESCRIÇÃO
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`Name`	O nome do agendamento.
`Frequency`	O tipo de frequência: Diária, Semanal ou Mensal.
`Day`	Se a frequência for diária.
`DaysInWeek`	Se a frequência for semanal.
`DayInMonth`	Se a frequência for mensal.
`WeekInMonth`	Se a frequência for mensal.
`StartDate`	O formato é `M/d/yy`
`StartTime`	A hora de início especificada como um relógio de 24 horas.
`FrequencyFactor`	Executar a cada n vezes, como todos os dias (valor = 1) ou em dias alternados (valor = 2)

PARÂMETRO	DESCRIÇÃO
`Description`	A descrição do backup agendado
`Enabled`	O parâmetro para habilitar este agendamento de backup. `True` quando habilitado e `false` quando desabilitado
`TimeZoneId`	O ID do fuso horário do Windows

Set-BckRstrSchedule

Modifica um agendamento de backup existente. Forneça o nome ou Uid para selecionar o agendamento a ser modificado.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.

PARÂMETRO	DESCRIÇÃO
`Quiet`	O parâmetro para suprimir a saída para o console.
`Name`	O nome do agendamento.
`Uid`	Se o nome do agendamento for alterado.
`Frequency`	O tipo de frequência: Diária, Semanal ou Mensal.
`Day`	Se a frequência for diária.
`DaysInWeek`	Se a frequência for semanal.
`DayInMonth`	Se a frequência for mensal.
`WeekInMonth`	Se a frequência for mensal.
`StartDate`	O formato é `M/d/yy`
`StartTime`	A hora de início especificada como um relógio de 24 horas.
`FrequencyFactor`	Executar a cada n vezes, como todos os dias (valor = 1) ou em dias alternados (valor = 2)
`Description`	A descrição do backup agendado
`Enabled`	O parâmetro para habilitar este agendamento de backup. `True` quando habilitado e `false` quando desabilitado
`TimeZoneId`	O ID do fuso horário do Windows

Set-BckRstrScheduleEnabled

Habilita um agendamento de backup existente. Forneça o nome ou Uid para selecionar o agendamento a ser habilitado.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`Name`	O nome do agendamento.
`Uid`	Se o nome do agendamento for alterado.

Set-BckRstrScheduleDisabled

Desabilita um agendamento de backup existente. Forneça o nome ou Uid para selecionar o agendamento a ser desabilitado.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`Name`	O nome do agendamento.
`Uid`	Se o nome do agendamento for alterado.

Cmdlet para limitar backups

Set-BckRstrOptions

Limita os backups agendados a um por dia para evitar backups idênticos.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`OneScheduledBackupPerDay`	O parâmetro para limitar backups agendados a um por dia para evitar backups idênticos.

Cmdlet de restauração

Restore-BckRstrBackups

Restaura membros de um único componente a partir de um backup existente.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do consumidor necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`BackupName`	O nome do backup. A extensão `.zip` é opcional.
`Component`	Os componentes a serem incluídos no backup.
`Notes`	As notas sobre o backup.
`CheckMode`	O parâmetro para identificar membros do componente que seriam restaurados, mas não executa a restauração real.
`RestoreType`	O tipo de restauração: MissingOnly ou MissingUpdateExisting

PARÂMETRO	DESCRIÇÃO
`IncludeByName`	O filtro para especificar quais membros do componente considerar para restauração. Esta é uma lista de valores de filtro separados por vírgulas e pode conter os caracteres curinga `*` e `?`.

Cmdlets de histórico

Get-BckRstrHistory

Obtém uma lista de detalhes do histórico para todas as ações.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.

PARÂMETRO	DESCRIÇÃO
`Quiet`	O parâmetro para suprimir a saída para o console.

Get-BckRstrSpecificBackupHistory

Obtém uma lista de detalhes do histórico para um backup específico.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`BackupName`	O nome do backup. A extensão `.zip` é opcional.

Set-BckRstrNotes

Define ou altera as notas em um registro de histórico.

Parâmetros:

PARÂMETRO	DESCRIÇÃO
`CustomerId`	O ID do cliente necessário para obter um token de portador.
`CientId`	O ID do cliente necessário para obter um token de portador.
`Secret`	O segredo necessário para obter um token de portador.
`CustomerInforFileSpec`	A especificação de arquivo totalmente qualificada do arquivo de informações do cliente contendo informações de segurança e ambiente.
`ProfileName`	O parâmetro para identificar um perfil de segurança existente usado no lugar dos parâmetros anteriores. Consulte XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud para saber como definir perfis de segurança.
`Environment`	O tipo de ambiente de produção: Production, ProductionGov, ProductionJP, OnPrem.
`Quiet`	O parâmetro para suprimir a saída para o console.
`BackupName`	O nome do backup. A extensão `.zip` é opcional.
`Notes`	As notas para definir ou alterar.

Solucionar problemas de configuração automatizada e informações adicionais

> **Importante:**
>
> Para mensagens de erro comuns para a Configuração Automatizada e soluções correspondentes, consulte as *Perguntas Frequentes sobre solução de problemas* no artigo do Knowledge Center CTX277730.

Erros da ferramenta de configuração automatizada

As operações da ferramenta de configuração automatizada podem, às vezes, produzir erros. Quando isso acontece, podem ocorrer falhas ao processar componentes como Catálogos de Máquinas, Grupos de Entrega ou Políticas de Grupo, por exemplo. O uso de `OnErrorAction` e parâmetros de continuação permite capturar erros no meio do processamento, resolvê-los e continuar de onde parou.

O valor padrão de `OnErrorAction` é `StopCompEnd`. Quando ocorre um erro, a ferramenta termina de processar o componente atual. Nenhum componente adicional é processado, e os erros não são propagados para componentes dependentes a jusante. Depois de resolver quaisquer erros, você pode executar novamente seus cmdlets com qualquer parâmetro de continuação aplicado.

Parâmetro OnErrorAction

Você pode definir valores de parâmetro `OnErrorAction` em comandos de migração para controlar como a ferramenta responde aos erros encontrados ao processar componentes.

Esta tabela mostra os valores dos parâmetros e suas descrições:

VALOR	DESCRIÇÃO
`Continue`	Tenta processar o maior número possível de todos os componentes.
`Pause`	Pausa no final do processamento e solicita que você continue ou pare.
`StopCompEnd`	Tenta processar o máximo possível do componente. Para depois que o componente é finalizado. (Padrão)
`StopImmediately`	O processamento para quando um erro é encontrado.

Cmdlets de migração

Você pode aplicar o parâmetro `OnErrorAction` aos seguintes comandos de migração:

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

Exemplo: `Merge-CvadAcToSite -OnErrorAction StopImmediately`

Parâmetros de retomada

Esses parâmetros definem como a ferramenta retoma depois que uma operação pausa ou para devido a um erro.

Você pode aplicar parâmetros de retomada a cmdlets de migração que incluem um dos seguintes valores de parâmetro `OnErrorAction`:

- `Pause`
- `StopCompEnd`
- `StopImmediately`

Esta tabela mostra os valores dos parâmetros e suas descrições:

VALOR	DESCRIÇÃO
`-AllRemaining`	Requer um componente inicial. O processamento começa no componente inicial e processa todos os componentes restantes. Vários componentes são processados.
`-Resume`	Usa o componente de `CurrentComponent.txt` como ponto de partida. Todos os restantes são definidos como verdadeiros. Vários componentes são processados.
`-Repeat`	Usa o componente de `CurrentComponent.txt` como ponto de

VALOR	DESCRIÇÃO
	partida. Todos os restantes são definidos como falsos. Apenas um componente é processado.

O último componente processado é armazenado no arquivo `CurrentComponent.txt` na pasta AutoConfig. Não é recomendável editar este arquivo. Se você especificar `-Resume` ou `-Repeat`, e `CurrentComponent.txt` estiver ausente ou for inválido, o processamento para e você é solicitado a selecionar um componente.

Definindo o OnErrorAction no arquivo CustomerInfo.yml

Você também pode definir valores `OnErrorAction` no arquivo `CustomerInfo.yml`. Defina os valores usando os seguintes cmdlets:

- Para um novo arquivo: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- Para um arquivo existente: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

Logs

A execução de qualquer cmdlet resulta na criação de um arquivo de log e em uma entrada no arquivo de log de histórico principal. Todos os arquivos de log de operação são colocados em uma pasta de backup. Todos os nomes de arquivo de log começam com `CitrixLog`, e então mostram a operação de configuração automática e a data e hora da execução do cmdlet. Os logs não são excluídos automaticamente.

O log de histórico principal está localizado em `*%HOMEPATH%\Documents\Citrix\AutoConfig*`, no arquivo chamado **History.Log**. Cada execução de cmdlet resulta em uma entrada de log principal contendo a data, operação, resultado, backup e locais dos arquivos de log da execução.

Você também pode usar o cmdlet `New-CvadAcZipInfoForSupport` para coletar logs e enviá-los à Citrix para suporte. Este cmdlet compacta todos os arquivos de log e .yml em um único arquivo zip. Informações confidenciais do cliente (CustomerInfo.yml e CvadAcSecurity.yml) não são incluídas no zip. O arquivo Icon.yml também é excluído devido ao seu tamanho. O arquivo zip é colocado em *%HOMEPATH%\Documents\Citrix\AutoConfig* e nomeado *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, com base na data e hora. Este arquivo zip também pode servir como backup.

Cada arquivo de log inclui o seguinte:

- O nome da operação e se o modo de verificação está ativado
- A data e hora de início e término
- Múltiplas entradas para as ações de cada componente e notificações de sucesso/falha
- Resumo das ações realizadas, incluindo várias contagens de objetos criados
- Correções sugeridas, quando aplicável
- Local da pasta de backup, quando aplicável
- Local do log principal
- Duração

Arquivos de diagnóstico

Os arquivos de diagnóstico ajudam a determinar e resolver problemas. Os seguintes arquivos são criados quando a operação é executada. Eles estão localizados na subpasta específica da ação em *%HOMEPATH%\Documents\Citrix\AutoConfig*. Inclua esses arquivos ao fornecer informações para o suporte de resolução de problemas.

Exportar

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

Este arquivo conta todas as chamadas do SDK do Broker PowerShell feitas para exportar a configuração do site para arquivos.

Importar, Mesclar, Restaurar, Sincronizar, Fazer backup, Comparar

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

Este arquivo documenta cada chamada da API Rest e informações relacionadas.

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

Este arquivo contém todo o conteúdo da API Rest `Add`, `Update` e `Delete`.

Problemas resultantes de dependências

Importações e mesclagens podem falhar devido a dependências ausentes. Alguns problemas comuns são:

1. As Políticas de Grupo estão sem filtros de grupo de entrega. As causas usuais são grupos de entrega que não foram importados.

2. Os aplicativos falham ao importar ou mesclar. A causa usual é a falta de grupos de entrega ou grupos de aplicativos que não foram importados.
3. Os grupos de aplicativos estão sem uma RestrictToTag. As causas usuais são tags que não foram importadas.
4. As conexões de host falham. A causa usual é a falta de informações de segurança no arquivo CvadAcSecurity.yml.
5. Os catálogos de máquinas falham. A causa usual são as conexões de host que não foram importadas.
6. Máquinas ausentes dos catálogos de máquinas e grupos de entrega. A causa usual são as máquinas que não foram encontradas no Active Directory.
7. Usuários ausentes dos grupos de entrega. A causa usual são os usuários que não foram encontrados no Active Directory.

Recomendações

- Não execute mais de uma instância da Configuração automatizada por vez. A execução de várias instâncias simultâneas produz resultados imprevisíveis no site da nuvem. Se isso ocorrer, execute novamente uma instância da Configuração automatizada para levar o site ao estado esperado.
- Não trabalhe nem altere dados no Studio enquanto a Configuração automatizada estiver em execução.
- Sempre verifique visualmente os resultados de mesclagem, importação ou restauração no Studio para garantir que o site da nuvem atenda às expectativas.

Pastas

Localização raiz da pasta padrão

Todas as operações da ferramenta de Configuração automatizada ocorrem na pasta raiz ou em subpastas dentro dela. A pasta raiz está localizada em *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Exportar

Todos os arquivos exportados são colocados em dois locais de pasta, proporcionando facilidade de uso e um histórico de exportações. As exportações são sempre colocadas na pasta raiz. As cópias são colocadas em uma subpasta chamada **Exportar** com a data e hora da exportação.

A pasta raiz sempre contém a configuração mais recente do site local exportado. Cada subpasta **Exportar** contém a exportação feita na data e hora indicadas, o que mantém um histórico de exportações. Você pode usar qualquer subpasta **Exportar** para configurar o site da nuvem. A Configuração automatizada não exclui nem modifica as subpastas de exportação existentes.

Importar/Mesclar/Sincronizar/Comparar

As operações `Import`, `Merge` e `Compare` são sempre originadas de arquivos localizados na pasta raiz. Cada operação resulta na criação de uma subpasta para a qual os arquivos da pasta raiz são copiados, fornecendo um histórico de arquivos de origem de alteração do site na nuvem.

Restaurar

A operação `Restore` usa uma subpasta existente para configurar o site na nuvem. A pasta de origem é especificada no parâmetro `-RestoreFolder` obrigatório. Ao contrário de outros comandos, nenhuma nova subpasta é criada porque a operação `Restore` usa uma subpasta existente. A pasta de restauração pode ser a pasta raiz, mas ainda deve ser especificada no parâmetro `-RestoreFolder`.

Backups

A Configuração Automatizada inicializa, atualiza e faz backup de uma configuração de site na nuvem. Com o tempo, muitas configurações diferentes podem mudar no site na nuvem. Para facilitar o uso a longo prazo e preservar as alterações do histórico, a Configuração Automatizada usa um esquema de preservação para salvar esse histórico de alterações e fornecer um método para restaurar estados anteriores.

Os backups de configuração do site na nuvem são sempre feitos em uma subpasta chamada **Backup** com a data e a hora do backup. A Configuração Automatizada não exclui nem modifica subpastas de exportação existentes.

Você pode usar os backups para restaurar componentes específicos ou sua configuração inteira. Para restaurar todo o grupo de entrega e os componentes do catálogo de máquinas, use o cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig/
Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **Nota:**

> As informações do arquivo de backup no cmdlet anterior são baseadas em seus próprios backups.

> Para restaurar toda a configuração do site na nuvem, use o cmdlet:

`Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss`

> **Nota:**
>
> As informações do arquivo de backup no cmdlet anterior são baseadas em seus próprios backups.

Alterando a pasta raiz padrão

As operações `Export`, `Import`, `Merge`, `Sync` e `Compare` podem alterar a pasta raiz padrão usando o parâmetro `–AlternateFolder`. A criação e o gerenciamento de subpastas por operação permanecem os mesmos conforme descrito anteriormente.

Arquivos copiados para subpastas

Todos os arquivos com extensão ".yml" são copiados para subpastas de operação, exceto os seguintes:

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

Backups automatizados de sites de nuvem à prova de falhas

Um backup da configuração atual do site de nuvem é feito antes de executar operações que alteram a configuração. Isso inclui os parâmetros `Import`, `Merge`, `Sync` e `Restore`. O backup está sempre em uma subpasta abaixo da subpasta operacional.

No caso de `Restore`, a pasta de backup é uma subpasta da pasta especificada no parâmetro `-RestoreFolder`.

Automação

Os cmdlets da ferramenta de configuração automatizada podem ser executados em scripts de automação sem intervenção do administrador, suprimindo os prompts e a exibição dos resultados do log na conclusão do cmdlet. Você também pode definir parâmetros para fazer o mesmo usando o arquivo CustomerInfo.yml.

Adicione o seguinte parâmetro aos cmdlets de modificação da nuvem para suprimir a exibição de prompts.

`-Confirm $false`

Adicione o seguinte parâmetro aos cmdlets para suprimir a exibição do log na conclusão do cmdlet.

`-DisplayLog $false`

Adicione o seguinte parâmetro aos cmdlets para suprimir o registro na janela de comando do PowerShell.

`-Quiet`

Como outro método, os seguintes parâmetros podem ser colocados no arquivo CustomerInfo.yml.

`Confirm: False`

`DisplayLog: False`

Exportando de PCs que não sejam o Delivery Controller™

A ferramenta de configuração automatizada usa vários SDKs do Citrix PowerShell para exportar a configuração do site local para arquivos. Esses SDKs são instalados automaticamente no Delivery Controller, permitindo que a ferramenta seja executada no Delivery Controller sem ações extras. Ao executar em máquinas que não são Delivery Controller, é necessário instalar o conjunto de SDKs do Citrix PowerShell necessários para a ferramenta. Este conjunto de SDKs faz parte do Citrix Studio, que pode ser instalado a partir da mídia de instalação do Citrix Virtual Apps and Desktops™.

> **Nota:**
>
> A configuração automatizada não pode ser executada no Cloud Connector.

Migrando para o Citrix Cloud™ Government e Japan Control Plane

Os ambientes Citrix Cloud Government e Japan Control Plane usam diferentes pontos de acesso para autenticar e alocar tokens de acesso. Este requisito exclusivo se aplica a qualquer ferramenta de configuração automatizada que acesse a nuvem. Execute as seguintes etapas para usar a configuração automatizada nesses ambientes.

1. Na pasta *%HOMEPATH%\Documents\Citrix\AutoConfig*, edite CustomerInfo.yml.
2. Adicione uma das seguintes linhas, dependendo do ambiente ao qual você deseja se conectar, ao CustomerInfo.yml (ou altere-a, se já estiver presente).

   ```
   Environment: 'ProductionGov'
   ```

   ou

   ```
   Environment: 'ProductionJP'
   ```

A Configuração Automatizada agora pode ser usada nesses ambientes.

Coleta de dados do Citrix Cloud

Para obter informações sobre quais dados o Citrix Cloud coleta, consulte Conteúdo do Cliente e Tratamento de Logs dos Serviços Citrix Cloud.

Recursos adicionais

Fórum de discussão

Visite o fórum de discussão da Citrix para Configuração Automatizada.

Vídeo

Assista a Por dentro da ferramenta de configuração automatizada para Citrix Virtual Apps and Desktops no YouTube.

Treinamento

O Cloud Learning Center contém guias de vídeo passo a passo para criar uma implantação de serviço, incluindo as tarefas descritas neste artigo. Consulte Caminho de Aprendizagem para Migrar Citrix Virtual Apps and Desktops para o Citrix Cloud.

Imprimir

Gerenciar impressoras em seu ambiente é um processo de várias etapas:

1. Familiarize-se com os conceitos de impressão, se ainda não o fez.
2. Planeje sua arquitetura de impressão. Isso inclui analisar suas necessidades de negócios, sua infraestrutura de impressão existente, como seus usuários e aplicativos interagem com a impressão hoje e qual modelo de gerenciamento de impressão melhor se aplica ao seu ambiente.
3. Configure seu ambiente de impressão selecionando um método de provisionamento de impressora e, em seguida, criando políticas para implantar seu design de impressão. Atualize as políticas quando novos funcionários ou servidores forem adicionados.
4. Teste uma configuração de impressão piloto antes de implantá-la para os usuários.
5. Mantenha seu ambiente de impressão Citrix® gerenciando drivers de impressora e otimizando o desempenho da impressão.
6. Solucione problemas que possam surgir.

Para obter informações completas sobre impressão em um ambiente Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops), comece com Imprimir. A partir desse artigo, você pode prosseguir para:

- Exemplos de configuração de impressão
- Melhores práticas
- Políticas e preferências de impressão
- Provisionar impressoras
- Manter o ambiente de impressão

Instalar o Universal Print Server em seus servidores de impressão

1. Certifique-se de que cada servidor de impressão tenha o Microsoft Virtual C++ Runtime 2017, 32 bits e 64 bits, instalado.

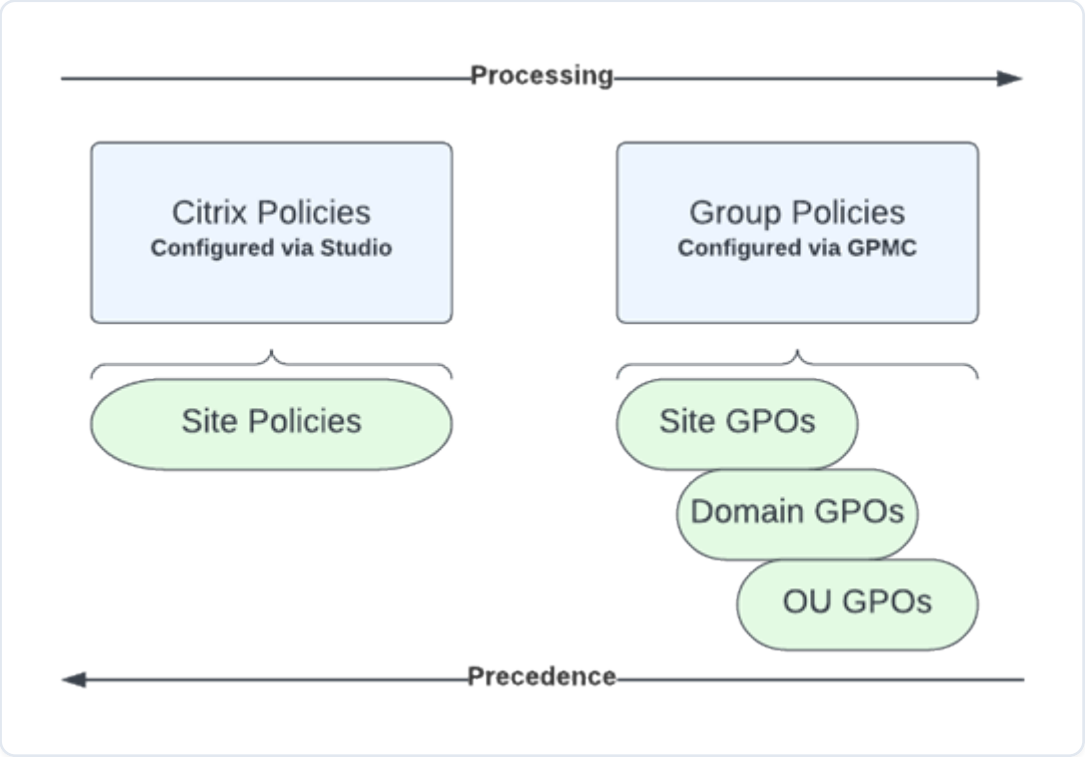
2. Navegue até a página de download do Citrix Universal Print Server e clique em **Download File**.
3. Execute um dos seguintes comandos em cada servidor de impressão:
    - Para um sistema operacional de 32 bits: **UpsServer_x86.msi**.
    - Para um sistema operacional de 64 bits: **UpsServer_x64.msi**.

Após instalar o Universal Print Server, configure-o usando as orientações em Provisionar impressoras.

Políticas

Políticas são uma coleção de configurações que definem como sessões, largura de banda e segurança são gerenciadas para um grupo de usuários, dispositivos ou tipos de conexão.

Você pode aplicar configurações de política a VDAs ou a usuários. Você pode editar as configurações no Web Studio ou nos objetos de política de grupo (GPOs) do Active Directory. Você pode especificar filtros (atribuições de objeto) para políticas. Se você não atribuir políticas especificamente a filtros, as configurações serão aplicadas a todas as sessões de usuário.



Você pode aplicar políticas em diferentes níveis da rede. As configurações de política colocadas no nível GPO da Unidade Organizacional têm a precedência mais alta na rede. As políticas no nível GPO do Domínio substituem as políticas no nível do Objeto de Política de Grupo do Site. O nível do Objeto de Política de Grupo do Site substitui quaisquer políticas conflitantes nos níveis de Políticas Locais da Microsoft e da Citrix.

Todas as Políticas de Site da Citrix são criadas e gerenciadas no console do Web Studio e armazenadas no Banco de Dados do Site. As Políticas de Grupo são criadas e gerenciadas usando o Console de Gerenciamento de Política de Grupo da Microsoft (GPMC) e armazenadas

no Active Directory. As Políticas Locais da Microsoft são criadas no Sistema Operacional Windows e são armazenadas no registro.

O Web Studio usa um Assistente de Modelagem para ajudar os administradores a comparar as configurações dentro de modelos e políticas para ajudar a eliminar configurações conflitantes e redundantes.

As configurações são mescladas de acordo com a prioridade e sua condição. Qualquer configuração desabilitada substitui uma configuração habilitada de classificação inferior. As configurações de política não configuradas são ignoradas e não substituem as configurações de classificação inferior.

As políticas do Web Studio também podem ter conflitos com as políticas de grupo no Active Directory, que podem se sobrepor dependendo da situação.

Todas as políticas são processadas na seguinte ordem:

1. No aplicativo Citrix Workspace™, o usuário final faz logon em um VDA usando credenciais de domínio.
2. As políticas da Citrix são processadas para o usuário final e para o VDA
3. As políticas são aplicadas na seguinte ordem:
    a. Políticas locais
    b. Políticas de site
    c. Políticas de domínio
    d. Políticas de UO (Unidade organizacional)

> **Nota:**

> - Nem todas as políticas podem estar presentes nos quatro níveis. Para a maioria dos clientes, apenas as políticas de site são usadas. As políticas locais exigem que o usuário faça logon no VDA para editar as políticas. Portanto, essas políticas quase nunca são usadas.
> - Não oferecemos suporte à mistura de políticas do Windows e do Citrix no mesmo GPO.

Visão geral

As políticas são uma coleção de configurações que definem como as sessões, a largura de banda e a segurança são gerenciadas para um grupo de usuários, dispositivos ou tipos de conexão. As políticas Citrix® fornecem uma maneira eficiente de gerenciar esses aspectos centralmente. Cada política pode incluir várias configurações e filtros (atribuições de objeto) adaptados ao seu ambiente.

Ferramentas para gerenciar políticas

- Studio

  As políticas criadas usando o Studio são armazenadas no plano de controle do DaaS, e as atualizações são enviadas para o VDA quando ocorre uma das seguintes situações:

  - Quando esse VDA se registra no plano de controle do DaaS
  - Quando um usuário inicia uma sessão

- Console de Gerenciamento de Política de Grupo (GPMC)

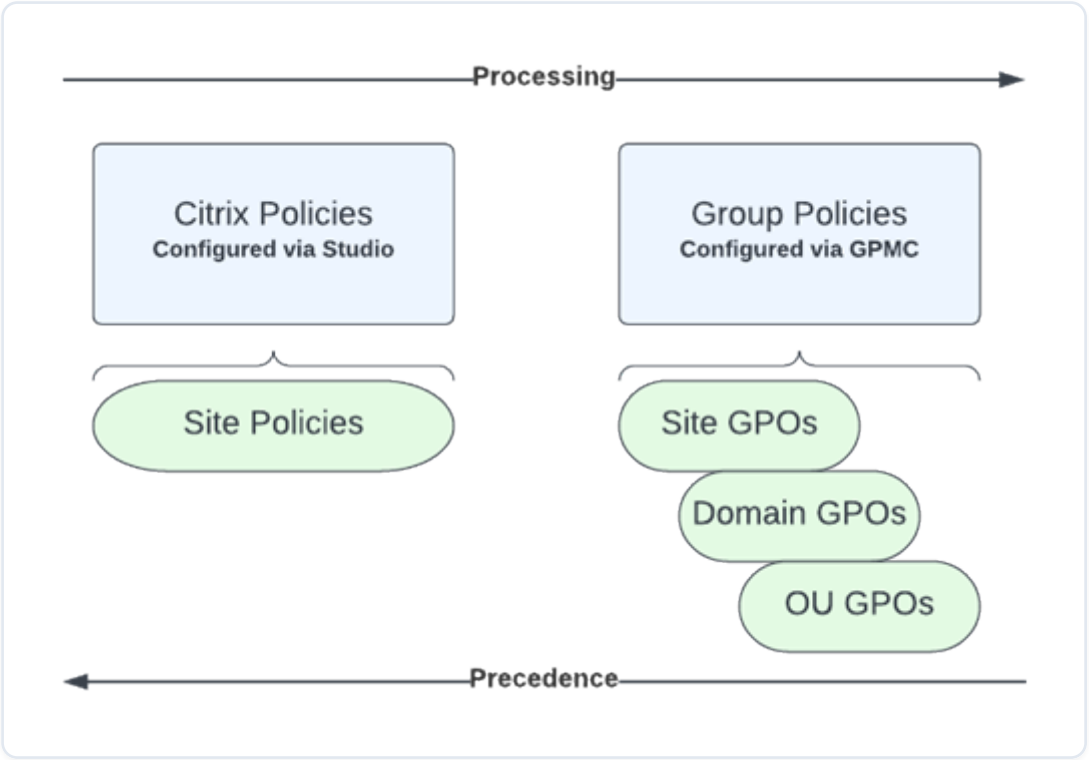
  Se o seu ambiente de rede usa o Active Directory e você tem permissão para gerenciar a política de grupo, você pode usar o GPMC para criar e editar políticas.

  No GPMC, você pode configurar Objetos de Política de Grupo (GPOs) com as configurações e filtros de que precisa. Essas políticas têm prioridade sobre as políticas configuradas no Studio. Para obter mais informações, consulte CTX238166.

Ordem de processamento da política

As configurações da política de grupo são processadas na seguinte ordem:

1. GPO de nível de site (armazenado no plano de controle do DaaS)
2. GPOs de nível de domínio
3. GPOs de Unidades Organizacionais (OU)



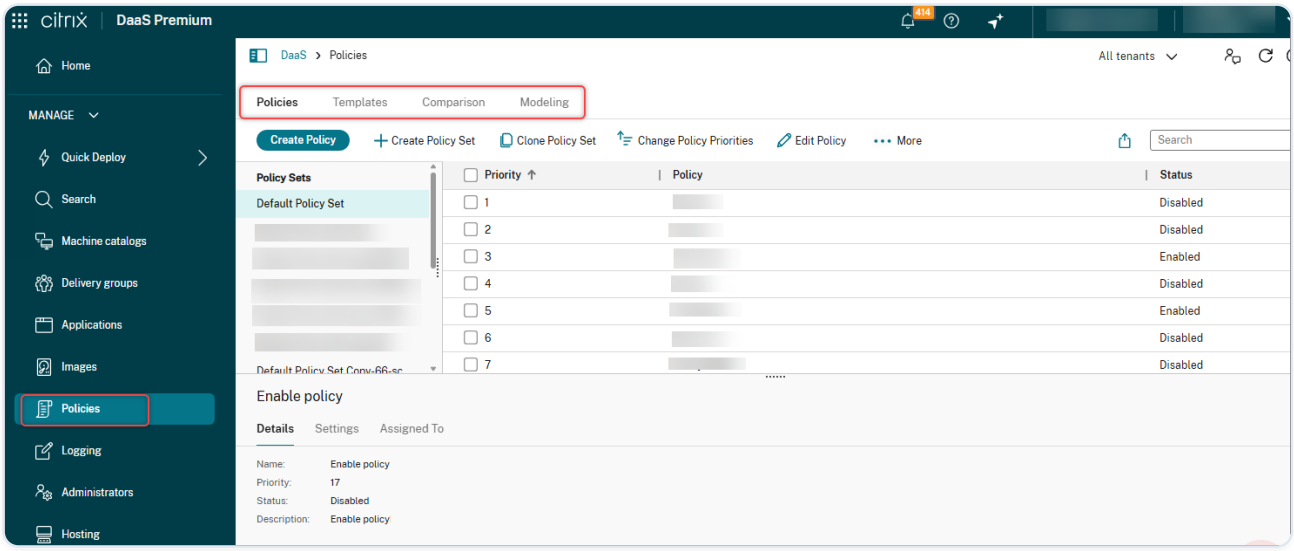
Se configurações diferentes forem aplicadas para a mesma política em dois GPOs, as configurações de política processadas por último sobrescrevem as configurações processadas anteriormente. Essa configuração significa que as configurações de política têm precedência na seguinte ordem:

1. GPOs de UO (prioridade mais alta)
2. GPOs de nível de domínio
3. GPOs de nível de site (prioridade mais baixa)

Se você estiver usando várias políticas com configurações conflitantes, você pode controlar a precedência atribuindo prioridades de política. Para obter mais informações, consulte Gerenciar cenários de política avançados.

Saiba mais sobre a interface Studio > Políticas

Para acessar políticas, configurações ou modelos, faça login no Studio e selecione **Políticas** no painel esquerdo.



- A guia **Políticas** permite criar e gerenciar conjuntos de políticas e políticas. Ao selecionar uma política de um conjunto de políticas, as seguintes guias aparecem:
  - **Visão geral** – Exibe o nome da política, prioridade, status e descrição.
  - **Configurações** – Lista todas as configurações configuradas.
  - **Atribuído a** – Mostra os grupos de entrega atribuídos. Você pode editar ou remover atribuições. As políticas são aplicadas com base no grupo de entrega da área de trabalho que executa a sessão. Para obter detalhes, consulte Criar políticas.
- A guia **Modelos** permite criar modelos de política e gerenciar modelos fornecidos pela Citrix e modelos personalizados. Ao selecionar um modelo, as seguintes guias aparecem:
  - **Descrição** – Explica a finalidade do modelo.
  - **Configurações** – Lista as configurações configuradas. Para obter detalhes, consulte Modelos de política.
- A guia **Comparação** permite comparar configurações em uma política ou modelo com outras. Use este recurso para verificar conformidade ou diferenças. Para obter detalhes, consulte Gerenciar cenários de política avançados.
- A guia **Modelagem** permite simular cenários de conexão e visualizar os resultados efetivos da política. Para obter detalhes, consulte Gerenciar cenários de política avançados.

Fluxo de trabalho de configuração de política

Para configurar políticas Citrix usando o Studio, siga este fluxo de trabalho:

1. Crie a política.
   a. Configure as configurações da política.

Adicione e configure as configurações necessárias para seu ambiente.

b. Atribua a política.

Atribua a política aos objetos de máquina e usuário apropriados.

2. Defina a prioridade da política.

   Organize as políticas em ordem de prioridade para determinar quais configurações têm precedência.

3. Verifique a política efetiva.

   Use o assistente de Modelagem de Política para confirmar as configurações aplicadas.

Criar modelos

Os modelos fornecem um ponto de partida predefinido para a criação de políticas. Oferecemos modelos integrados otimizados para ambientes e condições de rede específicos. Você pode usar esses modelos para:

- Crie suas próprias políticas e modelos para compartilhar entre sites.
- Referência durante comparações entre implantações. Por exemplo, “...ao usar o modelo Citrix X ou Y...”.
- Comunique as configurações de política com o Suporte Citrix ou terceiros confiáveis importando ou exportando modelos.

Modelos integrados

Os seguintes modelos integrados estão disponíveis:

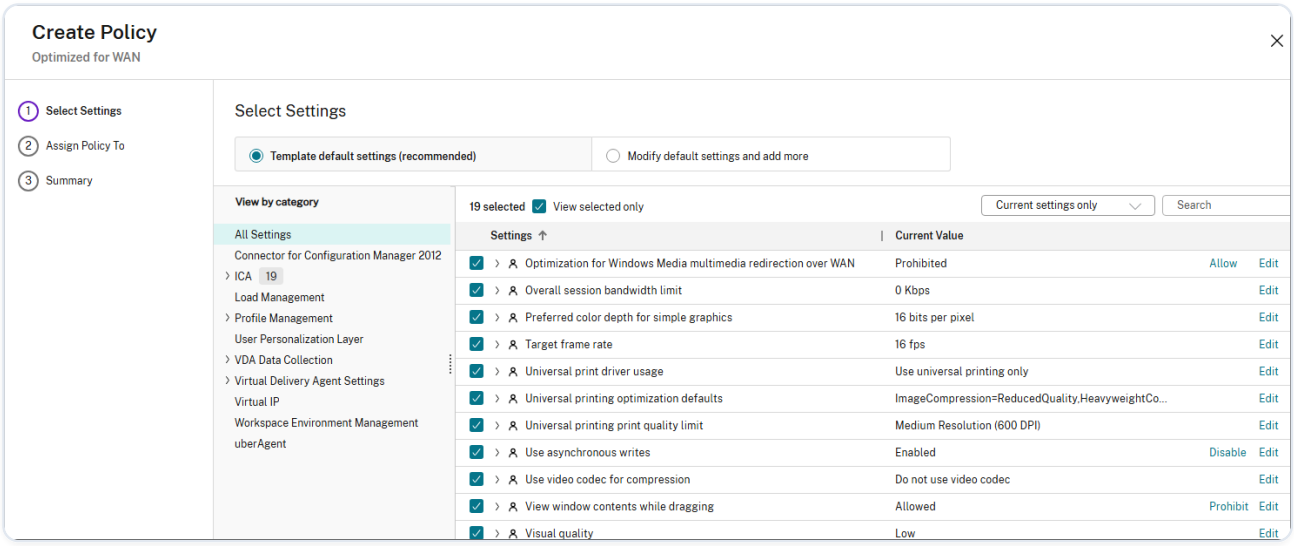
- **Experiência do usuário de altíssima definição**. Este modelo aplica configurações padrão que maximizam a experiência do usuário. Use este modelo em cenários onde várias políticas são processadas em ordem de precedência.
- **Alta escalabilidade do servidor**. Aplique este modelo para economizar recursos do servidor. Este modelo equilibra a experiência do usuário e a escalabilidade do servidor. Ele oferece uma boa experiência do usuário enquanto aumenta o número de usuários que você pode hospedar em um único servidor. Este modelo não usa um codec de vídeo para compactação de gráficos e impede a renderização multimídia no lado do servidor.
- **Alta escalabilidade do servidor - SO herdado**. Este modelo de alta escalabilidade do servidor se aplica apenas a VDAs que executam Windows Server 2008 R2 ou Windows 7 e

anteriores. Este modelo depende do modo gráfico herdado, que é mais eficiente para esses sistemas operacionais.

- **Otimizado para NetScaler SD-WAN.** Aplique este modelo para usuários que trabalham em filiais com NetScaler SD-WAN para otimizar a entrega de Citrix Virtual Desktops. (NetScaler SD-WAN é o novo nome para CloudBridge).
- **Otimizado para WAN**. Este modelo é destinado a trabalhadores de tarefas em filiais que usam WAN compartilhada ou locais remotos com conexões de baixa largura de banda. Os trabalhadores acessam aplicativos com interfaces de usuário graficamente simples e pouco conteúdo multimídia. Este modelo troca a experiência de reprodução de vídeo e alguma escalabilidade do servidor por eficiência de largura de banda otimizada.
- **Otimizado para WAN - SO herdado**. Este modelo se aplica apenas a VDAs que executam Windows Server 2008 R2 ou Windows 7 e anteriores. Este modelo depende do modo gráfico herdado, que é mais eficiente para esses sistemas operacionais.
- **Segurança e Controle**. Use este modelo em ambientes com baixa tolerância a riscos, para minimizar os recursos habilitados por padrão no Citrix DaaS. Este modelo inclui configurações que desabilitam o acesso ao seguinte:
  - Impressão
  - Área de transferência
  - Dispositivos periféricos
  - Mapeamento de unidades
  - Redirecionamento de porta
  - Aceleração de Flash em dispositivos de usuário

  A aplicação deste modelo pode usar mais largura de banda e reduzir a densidade de usuários por servidor.

Embora nós recomendemos usar as configurações padrão em modelos integrados, algumas configurações, como **Limite geral de largura de banda da sessão** nos **modelos WAN**, são deixadas sem configuração para permitir que os administradores façam ajustes específicos da implantação.



Considere que você está trabalhando com uma implantação (gerenciamento de políticas e VDAs) anterior ao XenApp e XenDesktop 7.6 FP3. Além disso, exige modelos de Alta Escalabilidade de Servidor e Otimizados para WAN. Neste caso, use as versões de SO herdadas desses modelos quando aplicável.

> **Nota:**
>
> Nós criamos e atualizamos modelos integrados. Você não pode modificar ou excluir esses modelos.

Criar modelos

Para criar um modelo a partir de um modelo:

1. No Studio, selecione **Políticas** no painel esquerdo.
2. Selecione a guia **Modelos** e, em seguida, selecione o modelo a partir do qual você cria o modelo.
3. Selecione a guia **Criar Modelo**. A tela **Selecionar Configurações** é exibida.
4. Selecione e configure as configurações de política a serem incluídas no modelo.
5. Clique em **Avançar**. A tela **Resumo** é exibida.
6. Insira um nome para o modelo.
7. Clique em **Concluir**. O novo modelo é exibido na guia **Modelos**.

Para criar um modelo com base em uma política:

1. No Studio, selecione **Políticas** no painel esquerdo.

2. Na guia **Políticas**, selecione a política a partir da qual você cria o modelo.
3. Clique na guia **Mais**.
4. Selecione **Salvar como Modelo**. A tela **Selecionar Configurações** é exibida.
5. Selecione e configure quaisquer novas configurações de política a serem incluídas no modelo.
6. Clique em **Avançar**. A tela **Resumo** é exibida.
7. Insira um nome e uma descrição para o modelo e, em seguida, clique em **Concluir**.

Criar políticas

Uma política define duas partes:

- Um grupo de configurações que definem como as sessões, largura de banda e segurança são gerenciadas para um grupo de usuários, dispositivos ou tipos de conexão.
- Usuários e máquinas aos quais a política será atribuída. Antes de criar uma política, decida qual grupo de usuários ou dispositivos ela afeta. Você pode querer criar uma política com base na função de trabalho, tipo de conexão, plataforma do dispositivo ou localização geográfica.

Ao criar uma política, você pode baseá-la em configurações de um modelo de política e personalizá-las conforme necessário. Você também pode começar do zero e adicionar manualmente as configurações necessárias. Esta seção aborda os seguintes tópicos:

- Como as políticas funcionam
- Criar políticas do zero
- Criar políticas a partir de modelos

> **Dica**

> Se uma política já existe para um grupo, considere editá-la em vez de criar uma nova. Evite criar políticas apenas para habilitar uma configuração específica ou excluir usuários específicos.

Como as políticas funcionam

Quando um usuário faz logon, todas as políticas que correspondem às atribuições para a conexão são identificadas. Essas políticas são classificadas por prioridade e múltiplas instâncias de qualquer configuração são comparadas. Para cada configuração, o valor da política de maior

prioridade é aplicado. Se uma política de maior prioridade desabilitar uma configuração, essa configuração substituirá qualquer política de menor prioridade onde ela estiver habilitada. As configurações que não são configuradas são ignoradas.

> **Importante:**
>
> Se você estiver configurando políticas do Active Directory e da Citrix usando o Console de Gerenciamento de Política de Grupo, as atribuições e configurações podem não ser aplicadas como esperado. Para obter mais informações, consulte CTX127461.

A política Não Filtrada

Fornecemos uma política padrão chamada **Não Filtrada**.

- Ao gerenciar políticas Citrix® no Web Studio, as configurações da política Não Filtrada se aplicam a todos os servidores, desktops e conexões no Site.
- Para que as configurações sejam aplicadas, o Site e as conexões devem estar dentro do escopo do GPO que contém a política.

  Exemplo: Um GPO chamado **Sales-US** está vinculado à OU **Sales** e inclui todos os membros da equipe de vendas dos EUA. Este GPO está configurado com uma política **Não Filtrada** com várias configurações de usuário. Quando um gerente de vendas faz logon, as configurações da política **Não Filtrada** são aplicadas porque o usuário está no GPO **Sales-US**.

Modos de atribuição

O modo de atribuição controla se uma política se aplica com base em como os critérios de conexão correspondem.

- **Permitir** (padrão): Aplica a política somente se a conexão corresponder aos critérios de atribuição.
- **Negar**: Aplica a política se a conexão não corresponder aos critérios.

Exemplo 1: Mesmo tipo de atribuição, modos diferentes

A Política 1 inclui:

- Atribuição A: Grupo de vendas, modo = Permitir
- Atribuição B: Conta do gerente de vendas, modo = Negar

Embora o usuário esteja no grupo de vendas, a atribuição Negar tem precedência. A política não se aplica quando o gerente de vendas faz logon.

Exemplo 2: Tipos de atribuição diferentes, mesmo modo

A Política 2 inclui:

- Atribuição C: Grupo de Vendas (Usuário), modo = Permitir
- Atribuição D: Intervalo de IP Corporativo (IP do Cliente), modo = Permitir

A política se aplica somente quando ambas as atribuições são satisfeitas. Se o gerente de vendas fizer logon do escritório, ambas as condições serão atendidas e a política será aplicada.

A Política 3 inclui:

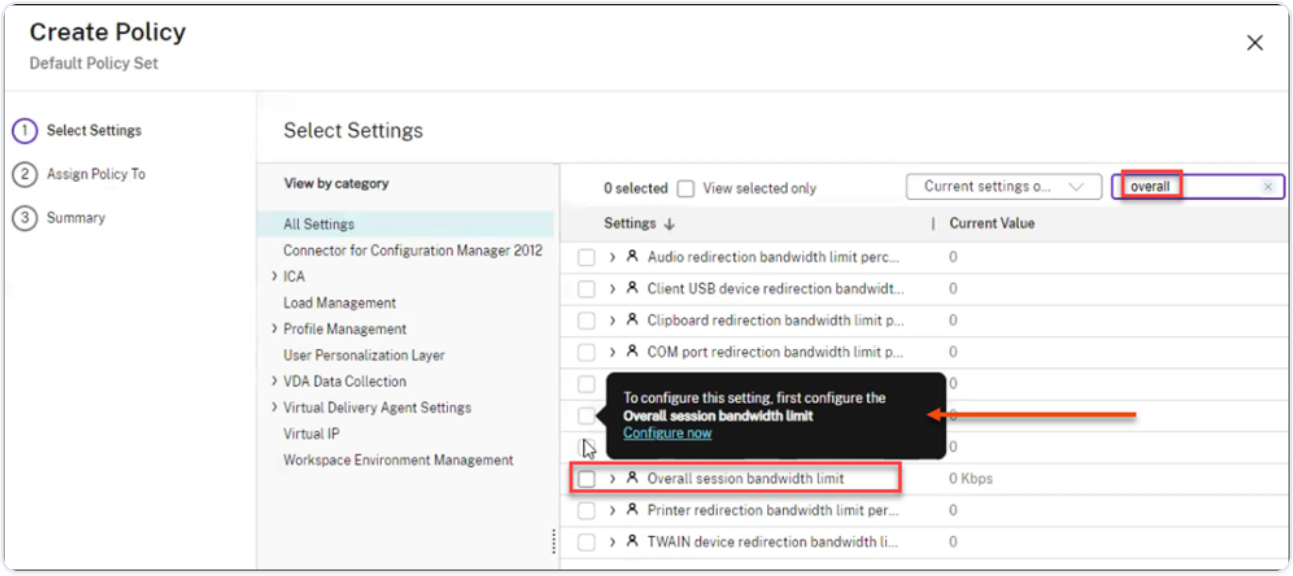
- Atribuição E: Grupo de Vendas (Usuário), modo = Permitir
- Atribuição F: Conexão do NetScaler Gateway (Controle de Acesso), modo = Permitir

Se o gerente de vendas fizer logon do escritório (não via NetScaler), a Atribuição F não será satisfeita, portanto, a política não se aplica.

Configurações de política: Relações pai-filho

Algumas configurações de política dependem de configurações pai. Por exemplo, você deve configurar **Limite geral de largura de banda da sessão** antes que suas configurações filhas se tornem disponíveis.

Ao configurar políticas no Web Studio, passe o mouse sobre uma configuração filha para ver qual pai deve ser configurado primeiro. Se um pai estiver desativado, as configurações filhas relacionadas serão automaticamente desativadas.



A tabela a seguir lista as configurações pai e suas configurações filhas correspondentes:

POLÍTICA PAI	POLÍTICAS FILHAS DEPENDENTES
Limite geral de largura de banda da sessão	Porcentagem de limite de largura de banda de redirecionamento de áudio
	Porcentagem de limite de largura de banda de redirecionamento da área de transferência
	Porcentagem de limite de largura de banda de redirecionamento de porta COM
	Porcentagem de limite de largura de banda de redirecionamento de arquivo
	Porcentagem de limite de largura de banda de aceleração multimídia HDX™ MediaStream
	Porcentagem de limite de largura de banda de redirecionamento de porta LPT
	Porcentagem de limite de largura de banda de redirecionamento de impressora
	Porcentagem de limite de largura de banda de redirecionamento de dispositivo USB do cliente
	Porcentagem do limite de largura de banda de redirecionamento de dispositivo TWAIN
Permitir redirecionamento de conteúdo bidirecional	URLs permitidas para serem redirecionadas para o Cliente
	URLs permitidas para serem redirecionadas para o VDA
Uso da CPU	Prioridade de processo excluída do uso da CPU
Modo gráfico legado	Nível de compressão progressiva
Habilitar marca d'água da sessão	Texto personalizado da marca d'água

POLÍTICA PAI	POLÍTICAS FILHAS DEPENDENTES
	Estilo da marca d'água da sessão
	Transparência da marca d'água
Transporte adaptável HDX	Modo tolerante a perdas para áudio

Estados das configurações de política

Algumas configurações de política podem ter um dos seguintes estados:

- **Permitido** ou **Proibido**: Permite ou impede a ação controlada pela configuração. Às vezes, os usuários são permitidos ou impedidos de gerenciar a ação da configuração em uma sessão. Por exemplo, se a animação do menu estiver definida como Permitido, os usuários podem controlá-la dentro de sua sessão.
- **Ativado** ou **Desativado**: liga ou desliga a configuração. Se uma configuração for desativada em uma política de prioridade mais alta, ela não será aplicada — mesmo que ativada em uma política de prioridade mais baixa.

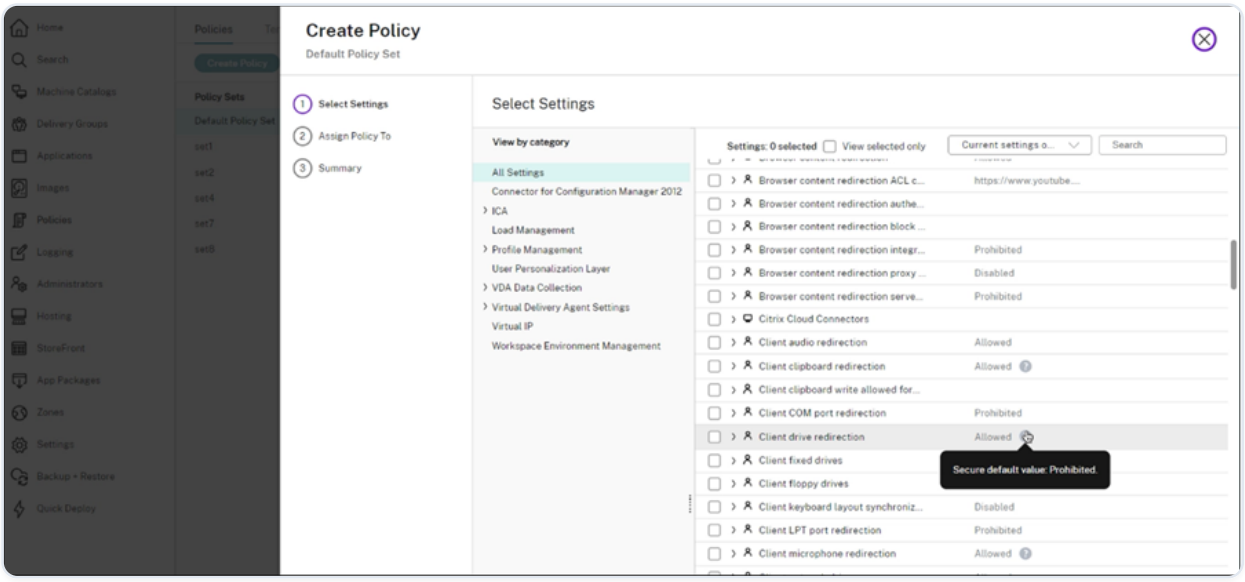
Configurações padrão seguras

Se a configuração padrão segura estiver ativada durante a instalação do VDA, a prioridade das configurações de política é a seguinte:

1. Configuração personalizada
2. Configuração padrão segura
3. Configuração padrão

Para visualizar o valor padrão seguro:

1. No Web Studio, clique em **Políticas** no painel esquerdo.
2. Na guia **Políticas**, clique em **Criar Política**.
3. Na tabela **Selecionar Configurações**, quando você passa o mouse sobre as configurações que têm **Permitido** como seu valor atual, é exibido **Valor padrão seguro: Proibido**.



Eficácia da configuração de política

Algumas configurações devem ser usadas e ativadas em conjunto. Por exemplo, para permitir que os usuários acessem unidades de rede em seu dispositivo local:

- **Redirecionamento de unidade cliente** deve ser ativado
- **Unidades de rede cliente** também devem ser incluídas

Se o **Redirecionamento de unidade cliente** estiver desativado, os usuários não poderão acessar unidades de rede mesmo que as **Unidades de rede cliente** estejam ativadas.

Em geral, as alterações nas configurações relacionadas à máquina entram em vigor quando o VDA é reiniciado ou um usuário faz logon. As alterações nas configurações relacionadas ao usuário são aplicadas no próximo logon.

Ao adicionar uma configuração a uma política, você pode selecionar Usar o valor padrão para evitar alterações. Esta opção desativa a configuração manual e aplica apenas o valor padrão, independentemente dos valores inseridos anteriormente.

Melhores práticas

- Atribua políticas a grupos em vez de usuários individuais. Se você atribuir políticas a grupos, as atribuições serão atualizadas automaticamente quando você adicionar ou remover usuários do grupo.
- Desative políticas não utilizadas. Políticas sem configurações adicionadas incorrem em sobrecarga de processamento desnecessária.

Criar políticas do zero

Para criar uma política:

1. No Web Studio, clique em **Políticas** no painel esquerdo.
2. Na guia **Políticas**, clique em **Criar Política**.
3. Na página **Selecionar Configurações**, selecione e configure as configurações e, em seguida, clique em **Avançar**.
4. Na página **Atribuir Política a**, selecione o conjunto de políticas onde esta política reside e, em seguida, selecione os objetos aos quais atribuir a política. Clique em **Avançar**.
5. Na página **Resumo**, preencha as seguintes configurações:
    a. Insira um nome e uma descrição para a política.
    b. Para habilitar a política, selecione **Habilitar política**.
6. Clique em **Concluir**.

Etapa 1: Selecionar e configurar as configurações da política

As configurações de política são agrupadas por função. Por exemplo, as configurações relacionadas ao Gerenciamento de Perfil estão na categoria **Gerenciamento de Perfil**.

Existem dois tipos de configurações:

- **Configurações do computador**: Aplicam-se a máquinas e entram em vigor quando o desktop virtual é iniciado (mesmo que nenhum usuário esteja logado). Elas definem os comportamentos do desktop virtual.
- **Configurações do usuário**: Aplicam-se quando um usuário se conecta ou reconecta. Elas definem a experiência do usuário.

Para selecionar e configurar uma configuração:

1. Na página **Selecionar Configurações**, para visualizar as configurações por versões de VDA, selecione uma das seguintes opções na lista suspensa no canto superior direito:
    - **Todas as configurações**: Visualizar todas as configurações para todas as versões de VDA
    - **Somente configurações atuais**: Visualize as configurações apenas para as versões atuais do VDA

- **Somente configurações legadas**: Visualize as configurações apenas para as versões VDA obsoletas

2. Para pesquisar uma configuração, digite o nome completo ou parcial da configuração na caixa de pesquisa.
3. Selecione uma configuração. Clique em **Habilitar** para ativá-la ou em **Editar** para especificar um valor.
4. Repita o passo 3 para selecionar e configurar mais configurações para a política.

> **Nota:**
>
> As configurações de política podem ser Habilitadas, Desabilitadas ou Não configuradas. Por padrão, as configurações de política não são configuradas, o que significa que não são adicionadas a uma política. As configurações são aplicadas somente quando são adicionadas a uma política.

Passo 2: Especificar atribuições de política

As atribuições de política definem a quais usuários e máquinas uma política se aplica. Para obter informações sobre como as atribuições afetam o comportamento da política, consulte Como as políticas funcionam.

Para especificar atribuições de política:

1. Na página **Atribuir Política a**, selecione **Usuários e computadores filtrados**.
2. Selecione os usuários ou computadores especificando atribuições (também conhecidas como *filtros*). Consulte a tabela a seguir para os tipos de atribuição disponíveis.

> **Nota:**
>
> - Se você não especificar nenhuma atribuição ou desativá-las, a política se aplicará a **todas** as conexões.
> - As *atribuições* de política também são conhecidas como *filtros* de política. Para obter mais informações, consulte Criar, modificar ou excluir um filtro para uma política e Como os filtros são aplicados?

TIPO DE ATRIBUIÇÃO	DESCRIÇÃO
Controle de Acesso	Condições de controle de acesso através das quais um cliente está se conectando • **Tipo de conexão**: Se a política deve ser aplicada a conexões feitas com ou sem o NetScaler® Gateway. *Nome do farm do NetScaler Gateway* - Nome do servidor virtual do NetScaler Gateway. *Condição de acesso* - Nome da política de análise de ponto de extremidade ou política de sessão a ser usada. • **Nome do farm do NetScaler Gateway**: Nome do servidor virtual do NetScaler Gateway. *Condição de acesso* - Nome da política de análise de ponto de extremidade ou política de sessão a ser usada. • **Condição de acesso**: Nome da política de análise de ponto de extremidade ou

TIPO DE ATRIBUIÇÃO	DESCRIÇÃO
	política de sessão a ser usada.
Citrix SD-WAN™	Se uma sessão de usuário é iniciada através do Citrix SD-WAN. **Nota:** Você pode adicionar apenas uma atribuição de Citrix SD-WAN a uma política.
Endereço IP do Cliente	Endereço IP do dispositivo do usuário usado para conectar-se à sessão: Exemplos de IPv4: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; Exemplos de IPv6: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Nome do Cliente	Nome do dispositivo do usuário. Correspondência exata: ClientABCName. Usando curinga: Client*Name.
Plataforma do Cliente	Tipo de SO do dispositivo do usuário usado para conectar a sessão, como Windows, Linux, iOS, Android ou HTML5. Versão VDA necessária: 2503 ou posterior.
Grupo de Entrega	Associação ao Grupo de Entrega.

TIPO DE ATRIBUIÇÃO	DESCRIÇÃO
Tipo de Grupo de Entrega	Tipo de desktop ou aplicativo: desktop privado, desktop compartilhado, aplicativo privado ou aplicativo compartilhado.
Unidade Organizacional (OU)	Unidade organizacional.
Tag	Tags. **Nota:** Aplique esta política a todas as máquinas marcadas. As tags de aplicativo não estão incluídas.
Usuário ou Grupo	Nome do usuário ou grupo. Os tipos de identidade suportados para usuários e grupos incluem Active Directory, Microsoft Entra ID, Okta e Google Cloud. Versão VDA necessária: 2507 ou posterior.

Criar políticas a partir de modelos

Você pode criar uma política com base em um modelo fornecido pela Citrix ou personalizado. A política resultante é independente do modelo original.

Para criar uma política a partir de um modelo:

1. No Web Studio, selecione **Políticas** no painel esquerdo.
2. Selecione a guia **Modelos** e, em seguida, selecione o modelo que deseja usar.
3. Clique em **Criar Política a partir do Modelo** na barra de ações. A página **Criar Política** é exibida, mostrando todas as configurações pré-configuradas no modelo selecionado.
4. Modifique as configurações e adicione mais configurações, se necessário, e, em seguida, clique em **Avançar**.

5. Na página **Atribuir Política a**, selecione o conjunto de políticas onde esta política reside e, em seguida, selecione os objetos aos quais atribuir a política. Clique em **Avançar**.
6. Na página **Resumo**, insira um nome e uma descrição para a política.
7. Clique em **Concluir**. A nova política aparece no conjunto de políticas especificado na guia **Políticas**.

Onde ir em seguida

- Priorizar políticas
- Simular e avaliar políticas

Criar conjuntos de políticas

Conjuntos de políticas são objetos no Citrix DaaS™ que agregam políticas para permitir acesso simplificado baseado em função e fácil gerenciamento. Uma vez criados, escopos e grupos de entrega são atribuídos a conjuntos de políticas para que apenas administradores autorizados possam gerenciar as políticas que se aplicam aos seus usuários e máquinas relevantes.

Conjuntos de políticas ajudam você a gerenciar políticas Citrix® de forma mais eficiente, organizando-as em grupos lógicos. Quando você atribui um conjunto de políticas a um grupo de entrega, o grupo de entrega usa apenas as políticas desse conjunto.

Esta seção explica como os conjuntos de políticas se comportam, como criá-los e atribuí-los, e como eles interagem com escopos e filtros.

Benefícios

Conjuntos de políticas oferecem vários benefícios importantes:

- Controle de acesso baseado em função para equipes de administradores distribuídas
- Fusões, aquisições e consolidações simplificadas
- Domínio de falha limitado
- Suporte multilocatário para políticas

A tabela a seguir compara como as políticas funcionam com e sem conjuntos de políticas:

SEM CONJUNTOS DE POLÍTICAS	COM CONJUNTOS DE POLÍTICAS
Todas as políticas, configurações, filtros (atribuições) e prioridades são gerenciados em um local central.	Cada conjunto de políticas tem suas próprias configurações, filtros (atribuições) e prioridades.
Se você gerencia uma política, você deve gerenciar todas as políticas.	Administradores completos podem delegar a administradores de nível inferior a capacidade de gerenciar um conjunto de políticas específico individualmente.
As políticas em ambientes grandes e distribuídos tornam-se complexas e difíceis de gerenciar.	As políticas em ambientes grandes e distribuídos podem ser divididas e gerenciadas facilmente.

Como funciona

Os conjuntos de políticas são atribuídos a grupos de entrega e têm escopo definido para administradores específicos. As políticas dentro de um conjunto continuam a usar filtros (atribuições) para determinar a quais usuários ou máquinas elas se aplicam.

Principais comportamentos:

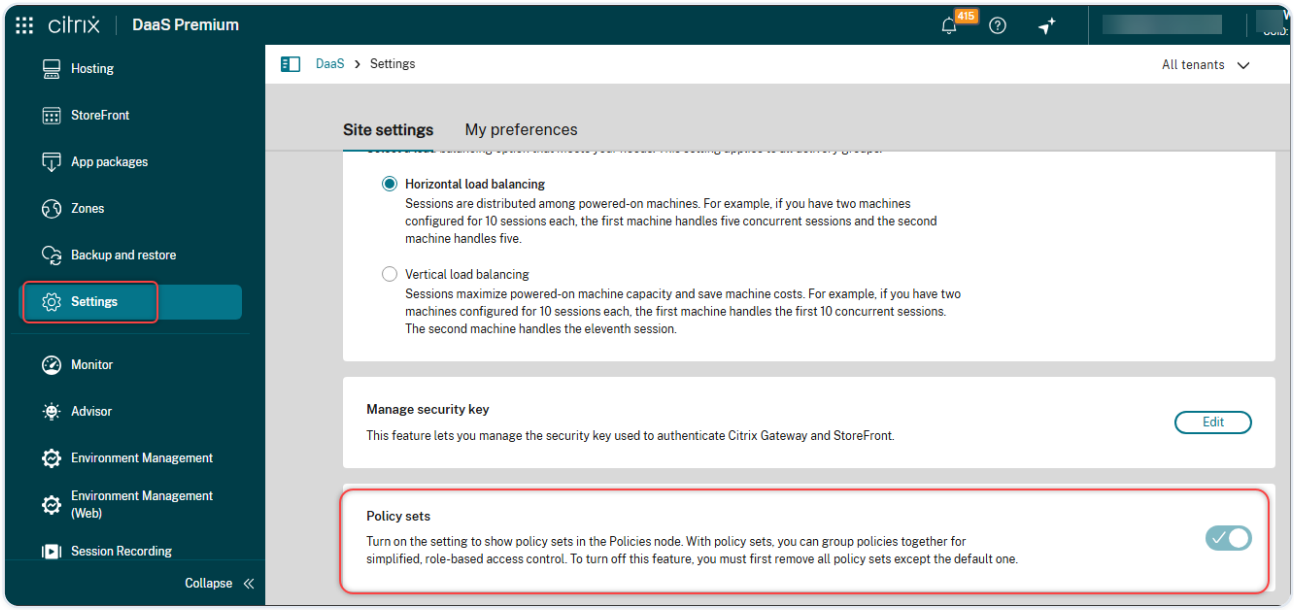
- Os conjuntos de políticas são atribuídos a grupos de entrega
  - Um grupo de entrega pode usar apenas um conjunto de políticas por vez.
  - Um conjunto de políticas pode ser atribuído a vários grupos de entrega.
  - Se um grupo de entrega não tiver um conjunto de políticas atribuído, ele usará o **Conjunto de Políticas Padrão**.
- Os filtros nas políticas ainda se aplicam, independentemente de a política estar em um conjunto.
- Um conjunto de políticas pode ter um ou vários escopos.
  - Um escopo representa uma coleção de objetos (por exemplo, conexões, catálogos, grupos de entrega e grupos de aplicativos) que os administradores podem gerenciar.
  - Como administradores, você pode definir o escopo do conjunto de políticas para que apenas administradores autorizados possam visualizá-lo ou editá-lo. Você pode definir escopos durante a criação do conjunto de políticas ou ao editar o conjunto posteriormente.

- O **Conjunto de Políticas Padrão** tem **Ignorar controle de escopo para este recurso** selecionado por padrão. Essa configuração garante que o conjunto de políticas permaneça visível para todos os administradores. Para aplicar o controle de escopo, edite o conjunto de políticas, desmarque a caixa de seleção **Ignorar controle de escopo para este recurso** e, em seguida, selecione os escopos desejados.

Os filtros e atribuições de políticas funcionam da mesma forma que sem conjuntos de políticas. Para obter mais informações, consulte Como os filtros são aplicados.

Habilitar conjuntos de políticas

No Studio, vá para **Configurações > Configurações do site** e ative a configuração **Conjuntos de políticas**.



Nota:

- Você deve habilitar os conjuntos de políticas antes de criar um conjunto de políticas.
- Quando você habilita os conjuntos de políticas, todas as políticas existentes são agrupadas no **Conjunto de Políticas Padrão**. Este conjunto é automaticamente atribuído a todos os grupos de entrega, a menos que você atribua um conjunto diferente. Depois que um novo conjunto de políticas é atribuído a um grupo de entrega, esse grupo para de usar o conjunto de políticas padrão.

Criar conjuntos de políticas

Você pode criar conjuntos de políticas para espelhar divisões lógicas em sua equipe de administradores e empresa. Por exemplo, você pode criar um conjunto de políticas para cada região geográfica, unidade de negócios ou para um caso de uso específico.

Você pode criar conjuntos de políticas de duas maneiras:

- Criar conjuntos de políticas do zero
- Criar um conjunto de políticas copiando um existente

Alternativamente, você pode usar as APIs REST do Citrix DaaS para criar e gerenciar conjuntos de políticas. Para obter mais informações, consulte Como criar um conjunto de políticas no Citrix DaaS.

Criar conjuntos de políticas do zero

1. No Studio, selecione o nó **Políticas** no painel esquerdo.
2. Clique na guia **Políticas**.
3. Selecione **Criar Conjunto de Políticas**.
4. Clique na guia **Nome e Descrição** e insira o nome e a descrição para o conjunto de políticas.
5. Clique na guia **Atribuições** e selecione um ou mais grupos de entrega.
6. Clique na guia **Escopos** e selecione os escopos que definem os objetos aos quais o conjunto de políticas pode ser aplicado.
7. Clique em **Criar** para finalizar.

Clonar conjuntos de políticas

1. No Studio, selecione o nó **Políticas** no painel esquerdo.
2. Clique na guia **Políticas**.
3. Selecione **Clonar Conjunto de Políticas**.
4. Atualize o nome do conjunto de políticas.
5. Atualize ou crie atribuições para o conjunto de políticas e clique em **Avançar**.
6. Selecione ou desmarque as políticas a serem incluídas no conjunto de políticas clonado.
7. Atualize o escopo da política.
8. Clique em **Criar**.

Priorizar políticas

Quando várias políticas se aplicam a uma conexão, o Citrix DaaS™ as avalia em ordem de prioridade. Um número menor significa uma prioridade mais alta (1 é a mais alta). Quando existem configurações conflitantes entre as políticas, a configuração da política de maior prioridade entra em vigor.

Você pode alterar a prioridade da política usando o Web Studio ou o PowerShell.

Alterar a prioridade da política usando o Web Studio

1. No **Web Studio**, selecione **Policies** no painel esquerdo.
2. Na guia **Policies**, selecione **Change Policy Priorities** na barra de ações.
3. Na página **Change Policy Priorities**, reordene as políticas usando qualquer um dos seguintes métodos:
    - Arraste uma política para a posição desejada.
    - Clique no ícone de seta **Up** ou **Down** para movê-la uma posição.
    - Clique no ícone de seta **Top** ou **Bottom** para movê-la para a primeira ou última posição.
    - Clique no ícone **Edit**, insira um número de prioridade e clique em **Save**.
4. Clique em **Save** para aplicar as alterações.

Gerenciar exceções de atribuição de política

Ao atribuir políticas a grupos de usuários, dispositivos de usuário ou máquinas usando filtros, alguns membros do grupo podem precisar de configurações diferentes. Você pode manipular esses casos sem criar políticas inteiramente separadas para cada indivíduo.

Você pode criar exceções para determinados usuários ou máquinas dentro de um grupo por:

- Criar uma política separada apenas para esses membros do grupo e dar a ela uma prioridade maior
- Usar o modo *Negar* para uma atribuição adicionada à política

Usar o modo Negar para exceções

Uma atribuição com o modo definido como *Negar* significa que a política se aplica a conexões que não correspondem aos critérios de atribuição. Por exemplo, uma política inclui as seguintes atribuições:

- *Atribuição A*: Intervalo de atribuição de endereço IP do cliente `208.77.88.*`, modo = *Permitir*.
- *Atribuição B*: Conta de usuário específica, modo = *Negar*.

Esta política se aplica aos usuários que se conectam do intervalo de IP especificado, **exceto** o usuário definido na *Atribuição B*.

> **Nota:**
>
> Na etapa **Atribuir Política**, se você desmarcar a caixa de seleção **Habilitar**, a atribuição será desabilitada. Se uma política não tiver atribuições habilitadas, ela se aplicará a todos os objetos no site.

Conteúdo relacionado

- Priorizar políticas
- Simular e avaliar políticas

Simular e avaliar políticas

Use as ferramentas de comparação e Modelagem de Políticas no Web Studio para verificar suas configurações, testar o comportamento da política e avaliar quais configurações se aplicam antes de implantá-las.

> **Nota:**
>
> - A guia **Modelagem** está disponível apenas se ativada por solicitação do cliente.
> - Apenas políticas ativadas com filtros são modeladas. Políticas desativadas nunca são aplicadas; políticas ativadas sem filtros são sempre aplicadas.

Comparar políticas e modelos

Use o recurso de comparação no Web Studio para visualizar as diferenças entre políticas, modelos ou configurações padrão. Isso ajuda você a verificar a consistência da configuração, manter a conformidade com as melhores práticas e solucionar comportamentos inesperados.

Você pode:

- Comparar as configurações de uma política ou modelo com outro
- Comparar configurações com valores padrão
- Identificar configurações conflitantes ou ausentes entre políticas

Para comparar políticas e modelos:

1. No Web Studio, selecione **Políticas** no painel esquerdo.
2. Clique na guia **Comparação** e, em seguida, clique em **Selecionar**.
3. Escolha as políticas ou modelos para comparar.
4. (Opcional) Selecione **Comparar com as configurações padrão** para incluir os padrões.
5. Clique em **Comparar**. As configurações aparecem em colunas.
    - Para ver todas as configurações, selecione **Mostrar Todas as Configurações**.
    - Para retornar à exibição padrão, selecione **Mostrar Configurações Comuns**.

Executar o assistente de Modelagem de Política

1. No Web Studio, selecione **Políticas**.
2. Selecione a guia **Modelagem**.
3. Selecione **Modelagem de Política** na barra de ações.
4. Leia a página **Introdução** e clique em **Avançar**.
5. Selecione usuários ou computadores. Você também pode procurar por contêineres ou usuários ou computadores específicos. Clique em **Avançar**.
6. Escolha sua evidência de filtro. Opcionalmente, refine a simulação especificando detalhes como **Grupo de entrega**, **Tags** e **Endereço IP do cliente**. Clique em **Avançar**.
7. Revise o resumo e clique em **Executar**.

Visualizar e gerenciar resultados de modelagem

Após a execução do assistente, ele gera um relatório que você pode revisar, agir e exportar.

Revisar o relatório

- Use o menu suspenso para visualizar **Todas as configurações**, **Configurações do computador** ou **Configurações do usuário**.
- Pesquise por configurações específicas.

- Clique em uma configuração para ver por que ela foi ou não foi aplicada.
- Exporte os resultados nos formatos JSON ou HTML.

Gerenciar o relatório

As seguintes opções estão disponíveis na barra de ações após a execução de uma simulação:

OPÇÃO	DESCRIÇÃO
Visualizar Relatório de Modelagem	Revise ou exporte os resultados.
Executar Modelagem de Política Novamente	Execute novamente usando os mesmos critérios.
Excluir Relatório de Modelagem	Remova o relatório atual.

Avaliar a aplicação de políticas usando o Conjunto Resultante de Políticas

Se uma conexão não se comportar como esperado, políticas conflitantes podem ser a causa. Políticas de prioridade mais alta podem substituir outras. Use o Conjunto Resultante de Política (RSoP) para avaliar quais configurações se aplicam a uma determinada conexão.

Dois métodos RSoP estão disponíveis:

- **Assistente de Modelagem de Política de Grupo Citrix**

  Simule um cenário de conexão especificando usuários e condições de atribuição.

- **Resultados da Política de Grupo**

  Gere um relatório das políticas Citrix aplicadas a um usuário e a um Virtual Delivery Agent (VDA).

> **Nota:**

> As configurações de política de site criadas no **Web Studio** não são incluídas no Conjunto Resultante de Política quando você executa o assistente de Modelagem de Política de Grupo Citrix a partir do Console de Gerenciamento de Política de Grupo (GPMC). Para obter os resultados mais abrangentes, inicie o assistente de Modelagem de Política a partir do **Web Studio**, a menos que você crie políticas usando apenas o GPMC.

Solucionar problemas de política

Usuários, endereços IP e outros objetos atribuídos podem ter várias políticas sendo aplicadas simultaneamente, o que pode levar a um comportamento inesperado.

Se você executar o assistente de Modelagem de Política e nenhuma política se aplicar às conexões de usuário, pode ser porque:

- Nenhuma política tem atribuições que correspondam aos critérios de avaliação.
- As políticas que correspondem à atribuição não têm configurações definidas.
- As políticas que correspondem à atribuição estão desabilitadas.

Para resolver esses problemas:

- Habilite as políticas relevantes.
- Configure pelo menos uma configuração para cada política.

> **Nota:**
>
> Em cenários de salto duplo (por exemplo, um VDA de SO de sessão única conectando-se a um VDA de SO de múltiplas sessões), as políticas Citrix tratam o VDA de SO de sessão única como o dispositivo do usuário. As imagens armazenadas em cache para o segundo salto se aplicam à máquina do primeiro salto.

Visualizar políticas aplicadas no Director

Não administradores podem usar o **Director** para visualizar as políticas que se aplicam a uma sessão de usuário. Isso é útil para verificar quais configurações de política estão em vigor sem exigir acesso ao Web Studio.

Referência de configurações de política

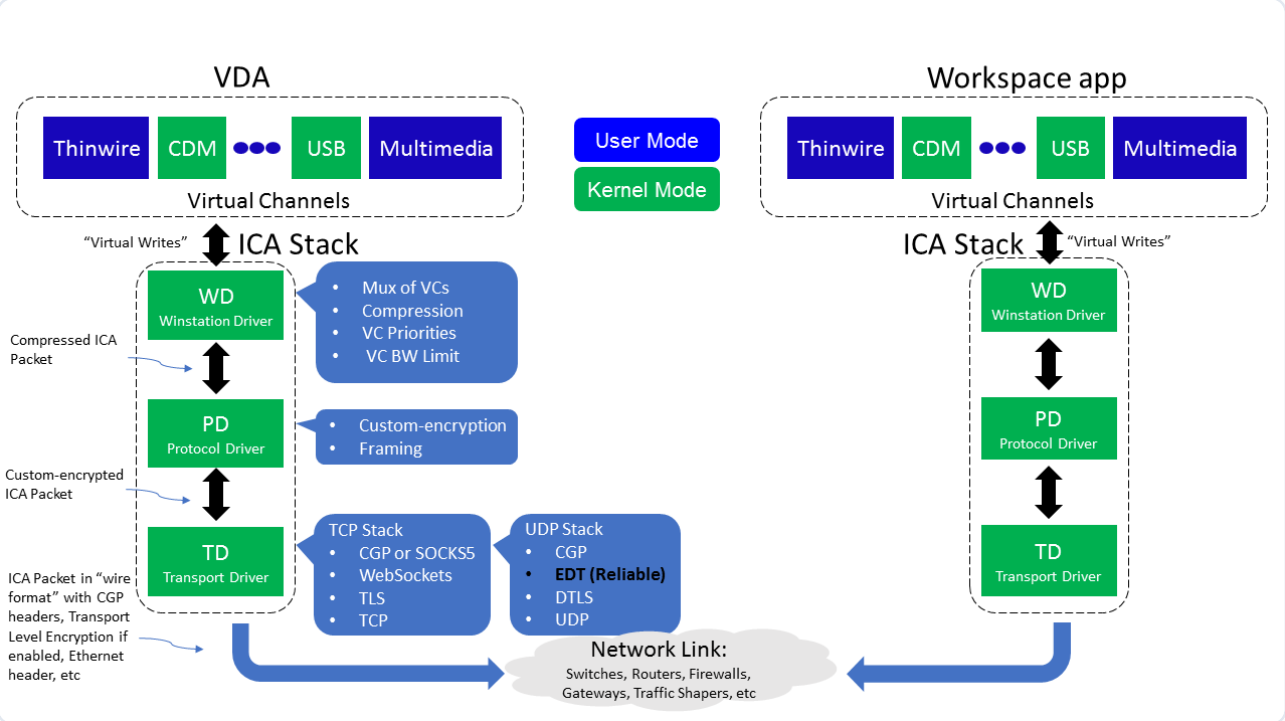
As configurações de política para Citrix DaaS™ são as mesmas que para Citrix Virtual Apps and Desktops™. Para obter mais informações, consulte Referência de configurações de política na documentação do Citrix Virtual Apps and Desktops.

Visão geral do HDX™

Aviso:

A edição incorreta do registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

O Citrix HDX representa um amplo conjunto de tecnologias que oferecem uma experiência de alta definição aos usuários de aplicativos e desktops centralizados, em qualquer dispositivo e em qualquer rede.

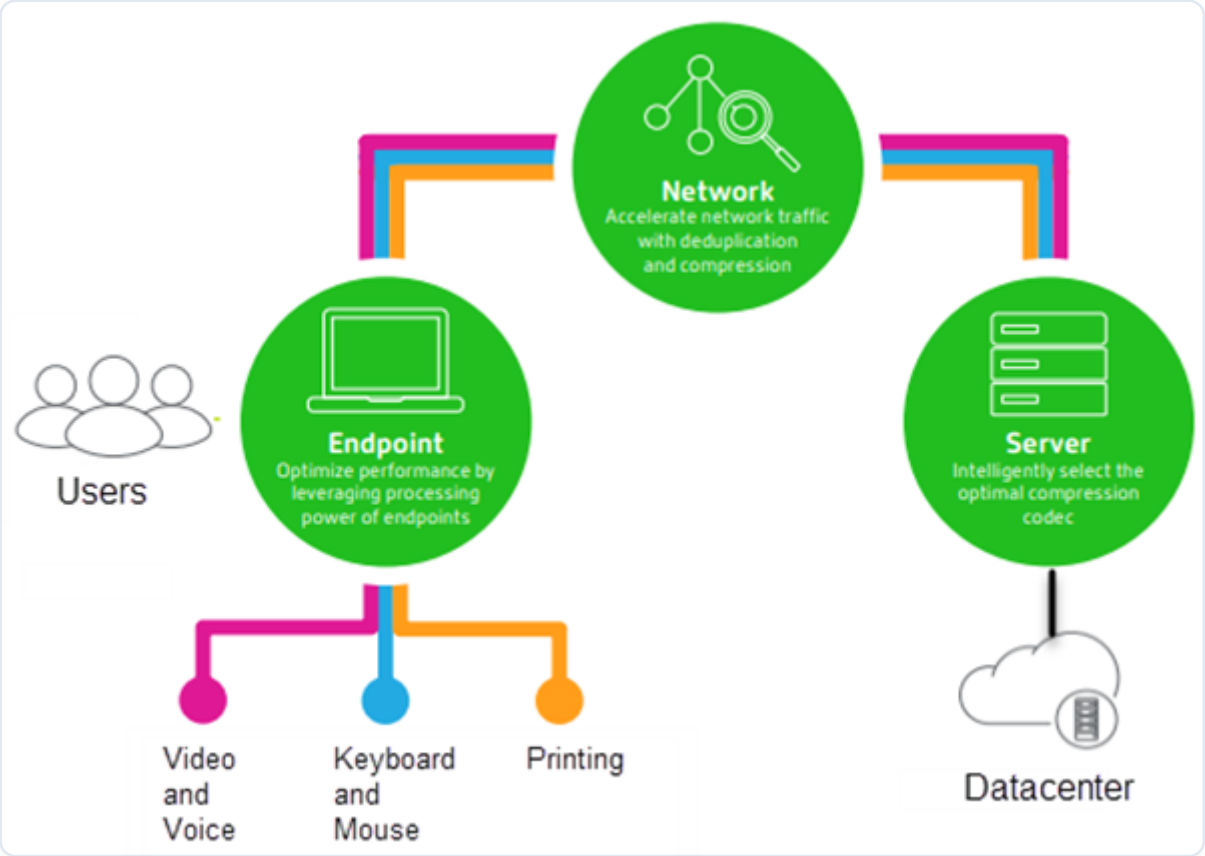


O HDX é projetado com base em três princípios técnicos:

- Redirecionamento inteligente
- Compressão adaptativa
- Desduplicação de dados

Aplicados em diferentes combinações, eles otimizam a experiência de TI e do usuário, diminuem o consumo de largura de banda e aumentam a densidade de usuários por servidor de hospedagem.

- **Redirecionamento inteligente** - O redirecionamento inteligente examina a atividade da tela, os comandos do aplicativo, o dispositivo de endpoint e os recursos de rede e servidor para determinar instantaneamente como e onde renderizar uma atividade de aplicativo ou desktop. A renderização pode ocorrer no dispositivo de endpoint ou no servidor de hospedagem.
- **Compressão adaptativa** - A compressão adaptativa permite que exibições multimídia ricas sejam entregues em conexões de rede com pouca largura de banda. O HDX primeiro avalia várias variáveis, como o tipo de entrada, dispositivo e exibição (texto, vídeo, voz e multimídia). Ele escolhe o codec de compressão ideal e a melhor proporção de uso de CPU e GPU. Em seguida, ele se adapta inteligentemente com base em cada usuário e situação únicos. Essa adaptação inteligente é por usuário, ou mesmo por sessão.



- **Desduplicação de dados** - A desduplicação do tráfego de rede reduz os dados agregados enviados entre cliente e servidor. Isso é feito aproveitando padrões repetidos em dados comumente acessados, como gráficos bitmap, documentos, trabalhos de impressão e mídia transmitida. O cache desses padrões permite que apenas as alterações sejam transmitidas pela rede, eliminando o tráfego duplicado. O HDX também suporta a transmissão multicast de fluxos de multimídia, onde uma única transmissão da fonte é visualizada por vários assinantes em um local, em vez de uma conexão um-para-um para cada usuário.

No dispositivo

O HDX usa a capacidade de computação dos dispositivos do usuário para aprimorar e otimizar a experiência do usuário. A tecnologia HDX garante que os usuários recebam uma experiência suave e contínua com conteúdo multimídia em seus desktops ou aplicativos virtuais. A reconexão de sessão permite que os usuários pausem desktops e aplicativos virtuais e retomem o trabalho de um dispositivo diferente do ponto onde pararam.

Na rede

O HDX incorpora recursos avançados de otimização e aceleração para oferecer o melhor desempenho em qualquer rede, incluindo conexões WAN de baixa largura de banda e alta latência.

Os recursos do HDX se adaptam às mudanças no ambiente. Os recursos equilibram desempenho e largura de banda. Eles aplicam as melhores tecnologias para cada cenário de usuário, seja o desktop ou aplicativo acessado localmente na rede corporativa ou remotamente de fora do firewall corporativo.

No data center

O HDX usa o poder de processamento e a escalabilidade dos servidores para oferecer desempenho gráfico avançado, independentemente dos recursos do dispositivo cliente.

O monitoramento de canal HDX fornecido pelo Citrix Director exibe o status dos canais HDX conectados nos dispositivos do usuário.

HDX Insight

O HDX Insight é a integração do NetScaler® Network Inspector e Performance Manager com o Director. Ele captura dados sobre o tráfego ICA e fornece uma visualização em painel de detalhes em tempo real e históricos. Esses dados incluem latência de sessão ICA do lado do cliente e do lado do servidor, uso de largura de banda dos canais ICA e o valor do tempo de ida e volta (round-trip time) do ICA de cada sessão.

Você pode habilitar o NetScaler para usar o canal virtual HDX Insight para mover todos os pontos de dados necessários em um formato não compactado. Se você desabilitar esse recurso, o dispositivo NetScaler descriptografa e descompacta o tráfego ICA® espalhado por vários canais

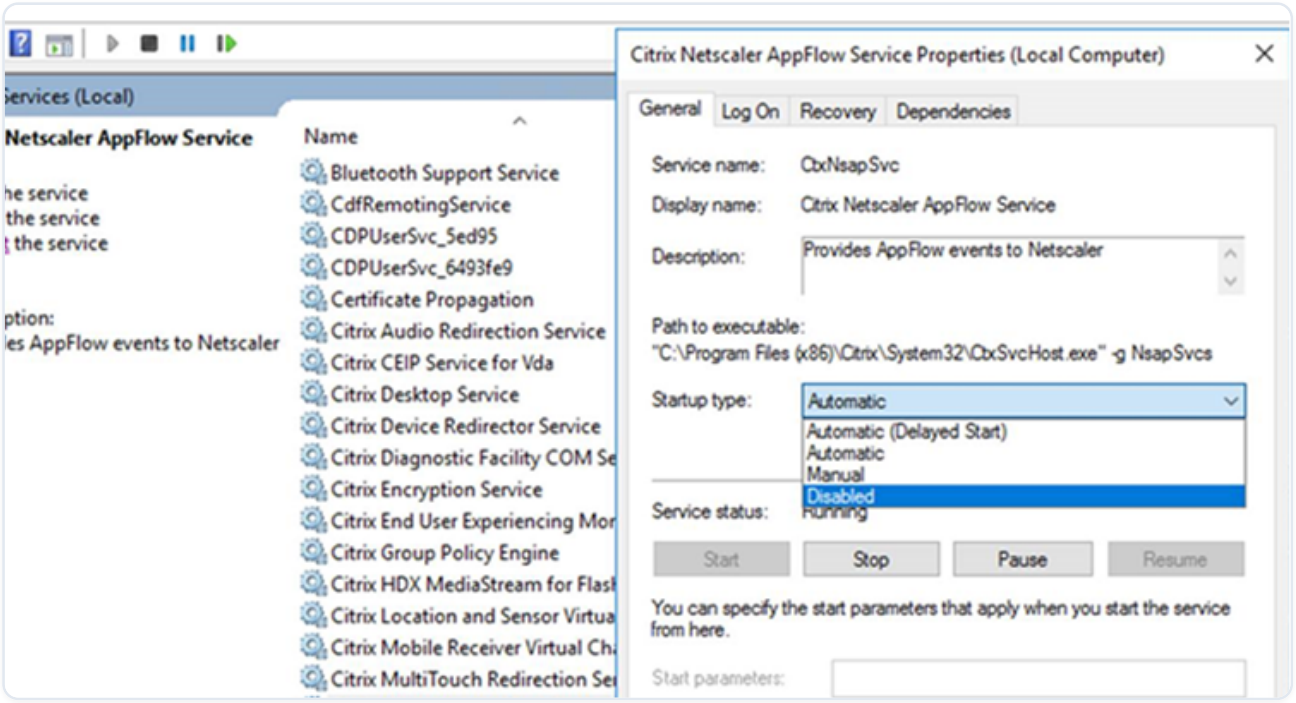
virtuais. Usar o canal virtual único diminui a complexidade, aumenta a escalabilidade e é mais econômico.

Requisitos mínimos:

- Citrix Virtual Apps e Desktops™ 7 v1808
- XenApp e XenDesktop 7.17
- NetScaler versão 12.0 Build 57.x
- Citrix Workspace™ app para Windows 1808
- Citrix Receiver para Windows 4.10
- Citrix Workspace app para Mac 1808
- Citrix Receiver para Mac 12.8

Habilitar ou desabilitar o canal virtual do HDX Insight

Para desabilitar este recurso, defina as propriedades do serviço Citrix NetScaler Application Flow como Desabilitado. Para habilitar, defina o serviço como Automático. Em ambos os casos, recomendamos que você reinicie a máquina do servidor após alterar essas propriedades. Por padrão, este serviço está habilitado (Automático).



Experimente os recursos do HDX a partir do seu desktop virtual

- Para ver como o redirecionamento de conteúdo do navegador, uma das quatro tecnologias de redirecionamento multimídia do HDX, acelera a entrega de conteúdo multimídia HTML5 e WebRTC:

  a. Baixe a extensão do navegador Chrome e instale-a no desktop virtual.

  b. Para experimentar como o redirecionamento de conteúdo do navegador acelera a entrega de conteúdo multimídia para desktops virtuais, assista a um vídeo em seu desktop a partir de um site que contenha vídeos HTML5, como o YouTube. Os usuários não sabem quando o redirecionamento de conteúdo do navegador está em execução. Para ver se o redirecionamento de conteúdo do navegador está sendo usado, arraste a janela do navegador rapidamente. Você verá um atraso ou fora do quadro entre a área de visualização e a interface do usuário. Você também pode clicar com o botão direito na página da web e procurar por **Sobre o Redirecionamento de Navegador HDX** no menu.

- Para ver como o HDX entrega áudio de alta definição:

  a. Configure seu cliente Citrix para máxima qualidade de áudio; consulte a documentação do Citrix Workspace app para obter detalhes.

  b. Reproduza arquivos de música usando um reprodutor de áudio digital (como o iTunes) em seu desktop.

O HDX oferece uma experiência superior de gráficos e vídeo para a maioria dos usuários por padrão, e a configuração não é necessária. As configurações de política do Citrix que fornecem a melhor experiência para a maioria dos casos de uso são habilitadas por padrão.

- O HDX seleciona automaticamente o melhor método de entrega com base no cliente, plataforma, aplicativo e largura de banda da rede, e então se autoajusta com base nas condições variáveis.
- O HDX otimiza o desempenho de gráficos 2D e 3D e vídeo.
- O HDX permite que os dispositivos do usuário transmitam arquivos multimídia diretamente do provedor de origem na internet ou intranet, em vez de através do servidor host. Se os requisitos para essa busca de conteúdo do lado do cliente não forem atendidos, a entrega de mídia retorna à busca de conteúdo do lado do servidor e ao redirecionamento multimídia. Geralmente, não são necessários ajustes nas políticas do recurso de redirecionamento multimídia.
- O HDX entrega conteúdo de vídeo rico renderizado pelo servidor para desktops virtuais quando o redirecionamento multimídia não está disponível: visualize um vídeo em um site que

contenha vídeos de alta definição, como `<http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>`.

É bom saber:

- Para obter informações de suporte e requisitos para os recursos do HDX, consulte o artigo Requisitos do sistema. Salvo indicação em contrário, os recursos do HDX estão disponíveis para máquinas Windows Multi-session OS e Windows Single-session OS compatíveis, além de desktops de Acesso Remoto a PC.
- Este conteúdo descreve como otimizar a experiência do usuário, melhorar a escalabilidade do servidor ou reduzir os requisitos de largura de banda. Para obter informações sobre como usar as políticas e configurações de política do Citrix, consulte a documentação Políticas do Citrix para esta versão.
- Para instruções que incluem a edição do registro, use com cautela: editar o registro incorretamente pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Reconexão automática do cliente e confiabilidade da sessão

Ao acessar aplicativos ou desktops hospedados, pode ocorrer interrupção da rede. Para ter uma reconexão mais suave, oferecemos reconexão automática do cliente e confiabilidade da sessão. Em uma configuração padrão, a confiabilidade da sessão é iniciada e, em seguida, a reconexão automática do cliente é acionada.

Reconexão automática do cliente:

A reconexão automática do cliente reinicia o mecanismo do cliente para reconectar a uma sessão desconectada. A reconexão automática do cliente fecha (ou desconecta) a sessão do usuário após o tempo especificado na configuração. Se a reconexão automática do cliente estiver em andamento, o sistema envia uma notificação de interrupção de rede de aplicativos e desktops ao usuário da seguinte forma:

- **Desktops.** A janela da sessão fica esmaecida e um cronômetro de contagem regressiva mostra o tempo até que as reconexões ocorram.
- **Aplicativos.** A janela da sessão é fechada e uma caixa de diálogo aparece para o usuário contendo um cronômetro de contagem regressiva mostrando o tempo até que as reconexões sejam tentadas.

Durante a reconexão automática do cliente, as sessões são reiniciadas esperando conectividade de rede. O usuário não pode interagir com as sessões enquanto a reconexão automática do cliente estiver em andamento.

Na reconexão, as sessões desconectadas se reconectam usando as informações de conexão salvas. O usuário pode interagir com os aplicativos e desktops normalmente.

Configurações padrão de reconexão automática do cliente:

- Tempo limite de reconexão automática do cliente: 120 segundos
- Reconexão automática do cliente: Ativada
- Autenticação de reconexão automática do cliente: Desativada
- Registro de reconexão automática do cliente: Desativado

Para obter mais informações, consulte Configurações de política de reconexão automática do cliente.

Confiabilidade da sessão:

A confiabilidade da sessão reconecta as sessões ICA de forma transparente em caso de interrupções de rede. A confiabilidade da sessão fecha (ou desconecta) a sessão do usuário após o tempo especificado na configuração. Após o tempo limite de confiabilidade da sessão, as configurações de reconexão automática do cliente entram em vigor, tentando reconectar o usuário à sessão desconectada. Quando a confiabilidade da sessão está em andamento, as notificações de interrupção de rede de aplicativos e desktops são enviadas ao usuário da seguinte forma:

- **Desktops.** A janela da sessão torna-se translúcida e um cronômetro de contagem regressiva mostra o tempo até que as reconexões ocorram.
- **Aplicativos.** A janela torna-se translúcida, juntamente com pop-ups de conexão interrompida da área de notificação.

Enquanto a confiabilidade da sessão estiver ativa, o usuário não poderá interagir com as sessões ICA. No entanto, as ações do usuário, como pressionamentos de tecla, são armazenadas em buffer por alguns segundos imediatamente após a interrupção da rede e retransmitidas quando a rede estiver disponível.

Na reconexão, o cliente e o servidor retomam no mesmo ponto em que estavam em sua troca de protocolo. As janelas da sessão perdem a translucidez e os pop-ups apropriados da área de notificação são exibidos para os aplicativos.

Configurações padrão de confiabilidade da sessão

- Tempo limite de confiabilidade da sessão: 180 segundos
- Nível de opacidade da interface do usuário de reconexão: 80%
- Conexão de confiabilidade da sessão: Habilitado
- Número da porta de confiabilidade da sessão: 2598

Para obter mais informações, consulte Configurações da política de confiabilidade da sessão.

NetScaler com reconexão automática do cliente e confiabilidade da sessão:

Se as políticas Multistream e Multiport estiverem habilitadas no servidor e qualquer uma ou todas estas condições forem verdadeiras, a reconexão automática do cliente não funcionará:

- A confiabilidade da sessão está desabilitada no NetScaler Gateway.
- Ocorre um failover no dispositivo NetScaler.
- O NetScaler SD-WAN é usado com o NetScaler Gateway.

Taxa de transferência adaptativa HDX

A taxa de transferência adaptativa HDX ajusta inteligentemente a taxa de transferência máxima da sessão ICA, ajustando os buffers de saída. O número de buffers de saída é inicialmente definido com um valor alto. Esse valor alto permite que os dados sejam transmitidos ao cliente de forma mais rápida e eficiente, especialmente em redes com alta latência. Proporcionar melhor interatividade, transferências de arquivos mais rápidas, reprodução de vídeo mais suave, maior taxa de quadros e resolução resulta em uma experiência de usuário aprimorada.

A interatividade da sessão é constantemente medida para determinar se algum fluxo de dados dentro da sessão ICA está afetando negativamente a interatividade. Se isso ocorrer, a taxa de transferência é diminuída para reduzir o impacto do grande fluxo de dados na sessão e permitir que a interatividade se recupere.

> **Importante:**

> A taxa de transferência adaptativa HDX altera a forma como os buffers de saída são definidos, movendo esse mecanismo do cliente para o VDA, e nenhuma configuração manual é necessária.

> Este recurso tem os seguintes requisitos:

- VDA versão 1811 ou posterior
- Aplicativo Workspace para Windows 1811 ou posterior

Melhorar a qualidade da imagem enviada para os dispositivos do usuário

As seguintes configurações de política de exibição visual controlam a qualidade das imagens enviadas de desktops virtuais para os dispositivos do usuário.

- Qualidade visual. Controla a qualidade visual das imagens exibidas no dispositivo do usuário: média, alta, sempre sem perdas, construir para sem perdas (padrão = média). A qualidade de vídeo real usando a configuração padrão de média depende da largura de banda disponível.
- Taxa de quadros alvo. Especifica o número máximo de quadros por segundo que são enviados do desktop virtual para o dispositivo do usuário (padrão = 30). Para dispositivos com CPUs mais lentas, especificar um valor menor pode melhorar a experiência do usuário. A taxa de quadros máxima suportada por segundo é 60.
- Limite de memória de exibição. Especifica o tamanho máximo do buffer de vídeo para a sessão em kilobytes (padrão = 65536 KB). Para conexões que exigem maior profundidade de cor e resolução mais alta, aumente o limite. Você pode calcular a memória máxima necessária.

Melhorar o desempenho da videoconferência

Vários aplicativos populares de videoconferência são otimizados para entrega a partir do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) através de redirecionamento multimídia (consulte, por exemplo, HDX RealTime Optimization Pack). Para aplicativos que não são otimizados, a compressão de vídeo da webcam HDX melhora a eficiência da largura de banda e a tolerância à latência para webcams durante videoconferências em uma sessão. Essa tecnologia transmite o tráfego da webcam por um canal virtual multimídia dedicado. Essa tecnologia usa menos largura de banda em comparação com o suporte de redirecionamento USB isócrono HDX Plug-n-Play e funciona bem em conexões WAN.

Os usuários do aplicativo Citrix Workspace podem substituir o comportamento padrão escolhendo a configuração de Microfone e Webcam do Desktop Viewer **Não usar meu microfone ou webcam**. Para evitar que os usuários alternem da compressão de vídeo da webcam HDX, desative o redirecionamento de dispositivo USB usando as configurações de política em Configurações de política ICA > Configurações de política de dispositivos USB.

A compressão de vídeo da webcam HDX exige que as seguintes configurações de política estejam ativadas (todas estão ativadas por padrão).

- Redirecionamento de áudio do cliente
- Redirecionamento de microfone do cliente
- Conferência multimídia
- Redirecionamento de Mídia do Windows

Se uma webcam suportar codificação de hardware, a compressão de vídeo HDX usará a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de banda do que a codificação de software. Para forçar a compressão de software, adicione o seguinte valor de chave DWORD à chave do registro: `HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1`.

Prioridades de tráfego de rede

As prioridades são atribuídas ao tráfego de rede em várias conexões para uma sessão usando roteadores compatíveis com Qualidade de Serviço. Quatro fluxos TCP e dois fluxos User Datagram Protocol (UDP) estão disponíveis para transportar o tráfego ICA entre o dispositivo do usuário e o servidor:

- Fluxos TCP - tempo real, interativo, em segundo plano e em massa
- Fluxos UDP - voz e acesso remoto de exibição Framehawk

Cada canal virtual é associado a uma prioridade específica e transportado na conexão correspondente. Você pode definir os canais independentemente, com base no número da porta TCP usado para a conexão.

Conexões de streaming de múltiplos canais são suportadas para Virtual Delivery Agents (VDAs) instalados em máquinas Windows 10 e Windows 8. Trabalhe com seu administrador de rede para garantir que as portas do Common Gateway Protocol (CGP) configuradas na definição da Política de Múltiplas Portas sejam atribuídas corretamente nos roteadores de rede.

A Qualidade de Serviço é suportada apenas quando várias portas de confiabilidade de sessão, ou as portas CGP, estão configuradas.

> **Aviso:**

> Use segurança de transporte ao usar este recurso. A Citrix recomenda usar o Internet Protocol Security (IPsec) ou o Transport Layer Security (TLS). As conexões TLS são suportadas apenas quando as conexões atravessam um NetScaler Gateway que suporta ICA multi-stream. Em uma rede corporativa interna, conexões multi-stream com TLS não são suportadas.

> Para definir a Qualidade de Serviço para múltiplas conexões de streaming, adicione as seguintes configurações de política Citrix a uma política (consulte Configurações de política de conexões multi-stream para obter detalhes):

- Política de Múltiplas Portas - Esta configuração especifica portas para o tráfego ICA em várias conexões e estabelece prioridades de rede.
  - Selecione uma prioridade na lista de prioridades da porta padrão CGP. Por padrão, a porta primária (2598) tem prioridade Alta.
  - Digite mais portas CGP em CGP port1, CGP port2 e CGP port3 conforme necessário, e identifique as prioridades para cada uma. Cada porta deve ter uma prioridade única.

  Configure explicitamente os firewalls nos VDAs para permitir o tráfego TCP adicional.
- Configuração de computador Multi-Stream - Esta configuração está desabilitada por padrão. Se você usa o Citrix NetScaler SD-WAN com suporte a Multi-Stream em seu ambiente, não precisa configurar esta definição. Configure esta definição de política ao usar roteadores de terceiros ou Branch Repeaters legados para alcançar a Qualidade de Serviço desejada.
- Configuração de usuário Multi-Stream - Esta configuração está desabilitada por padrão.

Para que as políticas que contêm essas configurações entrem em vigor, os usuários devem fazer logoff e, em seguida, logon na rede.

Mostrar ou ocultar a barra de idiomas remota

A barra de idiomas exibe o idioma de entrada preferencial em uma sessão de aplicativo. Se esse recurso estiver habilitado (padrão), você poderá mostrar ou ocultar a barra de idiomas na interface do usuário **Preferências Avançadas > Barra de idiomas** no aplicativo Citrix Workspace para Windows. Usando uma configuração de registro no lado do VDA, você pode desabilitar o controle do cliente sobre o recurso da barra de idiomas. Se esse recurso estiver desabilitado, a configuração da interface do usuário do cliente não terá efeito, e a configuração atual por usuário determinará o estado da barra de idiomas. Para obter mais informações, consulte Melhorar a experiência do usuário.

Para desabilitar o controle do cliente sobre o recurso da barra de idiomas a partir do VDA:

1. No editor de registro, navegar até `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`.
2. Crie uma chave de valor DWORD, SeamlessFlags, e defina-a como 0x40000.

Mapeamento de teclado Unicode

Os Citrix Receivers que não são Windows usam o layout de teclado local (Unicode). Se um usuário alterar o layout de teclado local e o layout de teclado do servidor (código de varredura), eles podem não estar sincronizados e a saída estará incorreta. Por exemplo, o Usuário1 altera o layout de teclado local de inglês para alemão. O Usuário1 então altera o teclado do lado do servidor para alemão. Mesmo que ambos os layouts de teclado sejam alemães, eles podem não estar sincronizados, causando uma saída de caractere incorreta.

Habilitar ou desabilitar o mapeamento de layout de teclado Unicode

Por padrão, o recurso está desabilitado no lado do VDA. Para habilitar o recurso, ative-o usando o editor de registro regedit no VDA. Adicione a seguinte chave de registro:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Name: EnableKlMap

Type: DWORD

Value: 1

Para desabilitar este recurso, defina **EnableKlMap** como 0 ou exclua a chave **CtxKlMap**.

Habilitar modo compatível de mapeamento de layout de teclado Unicode

Por padrão, o mapeamento de layout de teclado Unicode automaticamente 'engancha' algumas APIs do Windows para recarregar o novo mapa de layout de teclado Unicode quando você altera o layout do teclado no lado do servidor. Algumas aplicações não podem ser 'enganchadas'. Para manter a compatibilidade, você pode alterar o recurso para o modo compatível para oferecer suporte a essas aplicações não 'enganchadas'. Adicione a seguinte chave de registro:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nome: DisableWindowHook

Tipo: DWORD

Valor: 1

Para usar o mapeamento normal de layout de teclado Unicode, defina **DisableWindowHook** como 0.

Canais virtuais Citrix ICA®

Aviso:

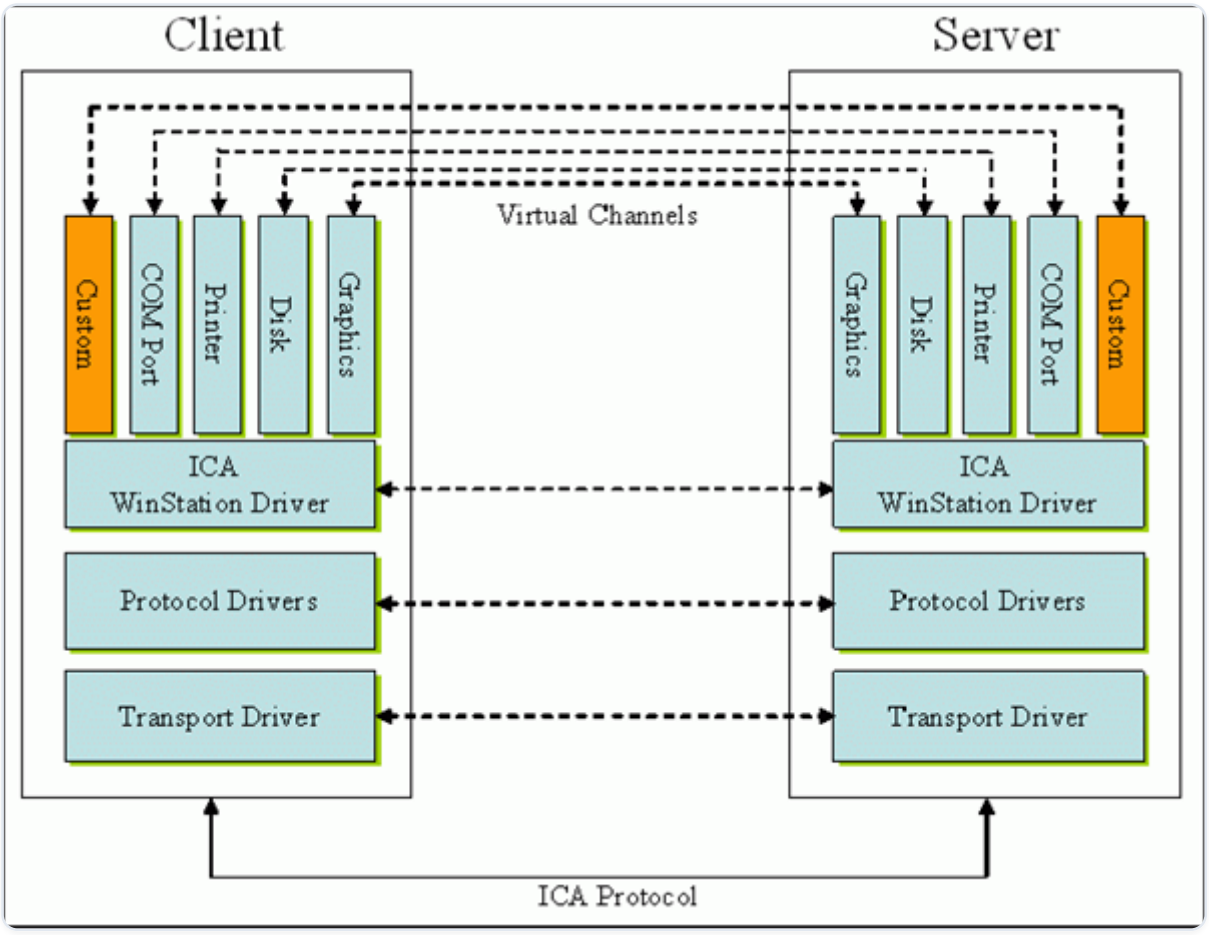
A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto de um Editor de Registro possam ser resolvidos. Use o Editor de Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

O que são canais virtuais ICA?

Uma grande parte da funcionalidade e comunicação entre o aplicativo Citrix Workspace™ e os servidores Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™) ocorre por meio de canais virtuais. Os canais virtuais são uma parte necessária da experiência de computação remota com os servidores Citrix DaaS. Os canais virtuais são usados para:

- Áudio
- Portas COM
- Discos
- Gráficos
- Portas LPT
- Impressoras
- Cartões inteligentes
- Canais virtuais personalizados de terceiros
- Vídeo

Novos canais virtuais são ocasionalmente lançados com os produtos Citrix DaaS™ e Citrix Workspace app para fornecer mais funcionalidade.



Um canal virtual consiste em um driver virtual do lado do cliente que se comunica com um aplicativo do lado do servidor. O Citrix DaaS é fornecido com vários canais virtuais incluídos. Eles são projetados para permitir que clientes e fornecedores terceirizados criem seus próprios canais virtuais usando um dos Kits de Desenvolvimento de Software (SDKs) fornecidos.

Os canais virtuais fornecem uma maneira segura de realizar várias tarefas. Por exemplo, um aplicativo que está sendo executado em um servidor Citrix Virtual Apps™ que se comunica com um dispositivo do lado do cliente ou um aplicativo que se comunica com o ambiente do lado do cliente.

No lado do cliente, os canais virtuais correspondem a drivers virtuais. Cada driver virtual fornece uma função específica. Alguns são necessários para a operação normal, e outros são opcionais. Os drivers virtuais operam no nível do protocolo da camada de apresentação. Pode haver vários protocolos ativos a qualquer momento, multiplexando canais fornecidos pela camada de protocolo da Windows Station (WinStation).

As seguintes funções estão contidas no valor do registro VirtualDriver sob este caminho de registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`

ou

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (para 64 bits)

- Thinwire3.0 (Obrigatório)
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- Clipboard
- ClientComm
- ClientAudio
- LicenseHandler (Obrigatório)
- TWI (Obrigatório)
- SmartCard
- ICACTL (Obrigatório)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Nota:**

> Você pode desabilitar funcionalidades específicas do cliente removendo um ou mais desses valores da chave do Registro. Por exemplo, se você quisesse remover a Área de Transferência do Cliente, remova a palavra **Clipboard**.

> Esta lista contém os arquivos de driver virtual do cliente e suas respectivas funções. O Citrix Virtual Apps e o aplicativo Citrix Workspace para Windows usam esses arquivos. Eles estão na forma de Bibliotecas de Vínculo Dinâmico (modo de usuário) e não de drivers do Windows (modo kernel), exceto para USB Genérico, conforme descrito em Canal virtual USB genérico.

- vd3dn.dll – Canal virtual Direct3D usado para redirecionamento de composição da área de trabalho
- vdcamN.dll – Áudio bidirecional
- vdcdm30n.dll – Mapeamento de unidade do cliente
- vdcom30N.dll - Mapeamento de porta COM do cliente
- vdcpm30N.dll – Mapeamento de impressora cliente
- vdctln.dll – Canal de controles ICA
- vddvc0n.dll – Canal virtual dinâmico
- vdeuemn.dll - Monitoramento da experiência do usuário final
- vdgusbn.dll – Canal virtual USB genérico
- vdkbhook.dll – Passagem transparente de teclas
- vdlfpn.dll – Canal de exibição Framehawk sobre transporte tipo UDP
- vdmmn.dll – Suporte multimídia
- vdmrvc.dll – Canal virtual do Mobile Receiver
- vdmtchn.dll - Suporte multitoque
- vdscardn.dll – Suporte a smartcard
- vdsens.dll – Canal virtual de sensores
- vdspl30n.dll – UPD do cliente
- vdsspin.dll – Kerberos
- vdtuin.dll – UI transparente
- vdtw30n.dll – Thinwire do Cliente
- vdtwin.dll – Seamless
- vdtwn.dll – Twain

Alguns canais virtuais são compilados em outros arquivos. Por exemplo, o Mapeamento da Área de Transferência está disponível em wfica32.exe

Compatibilidade de 64 bits

O aplicativo Citrix Workspace para Windows é compatível com 64 bits. Assim como a maioria dos binários compilados para 32 bits, esses arquivos de cliente têm equivalentes compilados para 64 bits:

- brapi64.dll

- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

Canal virtual USB genérico

A implementação do canal virtual USB genérico usa dois drivers de modo kernel junto com o driver de canal virtual vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

Como os canais virtuais ICA funcionam

Os canais virtuais são carregados de várias maneiras. O Shell (WfShell para o servidor e PicaShell para a estação de trabalho) carrega alguns canais virtuais. Alguns canais virtuais são hospedados como serviços do Windows.

Módulos de canal virtual carregados pelo Shell, por exemplo:

- EUEM
- Twain
- Área de Transferência
- Multimídia
- Compartilhamento de sessão contínuo
- Fuso Horário

Alguns são carregados como modo kernel, por exemplo:

- CtxDvcs.sys – Canal virtual dinâmico
- Icausbb.sys – Redirecionamento USB genérico
- Picadm.sys – Mapeamento de unidade do cliente
- Picaser.sys – Redirecionamento de porta COM
- Picapar.sys – Redirecionamento de porta LPT

Canal virtual gráfico no lado do servidor

A partir do XenApp 7.0 e XenDesktop 7.0, `ctxgfx.exe` hospeda o canal virtual gráfico para sessões baseadas em estação de trabalho e servidor de terminal. `Ctxgfx` hospeda módulos específicos da plataforma que interagem com o driver correspondente (`Icardd.dll` para RDSH e `vdod.dll` e `vidd.dll` para estação de trabalho).

Para implantações do XenDesktop® 3D Pro, um driver gráfico OEM é instalado para a GPU correspondente no VDA. `Ctxgfx` carrega módulos adaptadores especializados para interagir com o driver gráfico OEM.

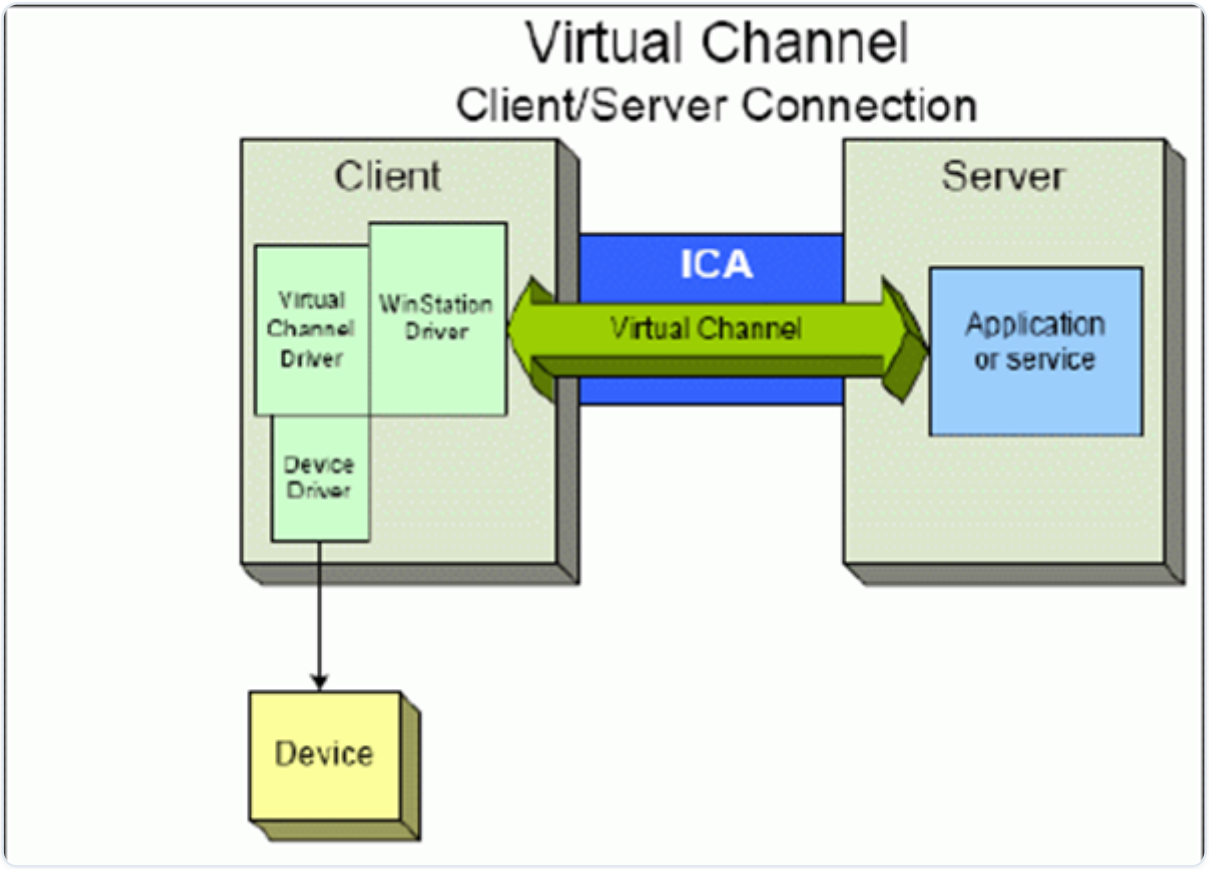
Hospedagem de canais especializados em serviços do Windows

Nos servidores Citrix DaaS, vários canais são hospedados como serviços do Windows. Essa hospedagem fornece semântica de um para muitos para várias aplicações em uma sessão e várias sessões no servidor. Exemplos de tais serviços incluem:

- Serviço de Redirecionamento de Dispositivo Citrix
- Serviço de Canal Virtual Dinâmico Citrix
- Serviço de Monitoramento da Experiência do Usuário Final Citrix
- Serviço de Canal Virtual de Localização e Sensor Citrix
- Serviço de Redirecionamento Multitoque Citrix
- Serviço de Gerenciador de Impressão Citrix
- Serviço de Smartcard Citrix
- Serviço de Redirecionamento de Áudio Citrix (somente Citrix Virtual Desktops™)
- Serviço de Canal de Status ICA Citrix

O canal virtual de áudio no Citrix Virtual Apps é hospedado usando o serviço de Áudio do Windows.

No lado do servidor, todos os canais virtuais do cliente são roteados através do driver WinStation, Wdica.sys. No lado do cliente, o driver WinStation correspondente, integrado ao wfica32.exe, pesquisa os canais virtuais do cliente. Esta imagem ilustra a conexão cliente-servidor do canal virtual.



Esta visão geral contém uma troca de dados cliente-servidor usando um canal virtual.

1. O cliente se conecta ao servidor Citrix DaaS. O cliente passa informações sobre os canais virtuais que ele suporta para o servidor.
2. O aplicativo do lado do servidor é iniciado, obtém um manipular para o canal virtual e, opcionalmente, consulta informações adicionais sobre o canal.
3. O driver virtual do cliente e o aplicativo do lado do servidor passam dados usando os dois métodos a seguir:

    - Se o aplicativo do servidor tiver dados para enviar ao cliente, os dados serão enviados ao cliente imediatamente. Quando o cliente recebe os dados, o driver WinStation desmultiplexa os dados do canal virtual do fluxo ICA e os passa imediatamente para o driver virtual do cliente.
    - Se o driver virtual do cliente tiver dados para enviar ao servidor, os dados serão enviados na próxima vez que o driver WinStation o pesquisar. Quando o servidor recebe os dados,

eles são enfileirados até que o aplicativo do canal virtual os leia. Não há como alertar o aplicativo do canal virtual do servidor de que os dados foram recebidos.

4. Quando o aplicativo de canal virtual do servidor é concluído, ele fecha o canal virtual e libera todos os recursos alocados.

Criando seu próprio canal virtual usando o SDK de Canal Virtual

A criação de um canal virtual usando o SDK de Canal Virtual requer conhecimento de programação intermediário. Use este método para fornecer um caminho de comunicação principal entre o cliente e o servidor. Por exemplo, se você estiver implementando o uso de um dispositivo no lado do cliente, como um scanner, para ser usado com um processo na sessão.

Nota:

- O SDK de Canal Virtual requer o SDK WFAPI para escrever o lado do servidor do canal virtual.
- Devido à segurança aprimorada para o Citrix DaaS, você deve especificar quais canais virtuais podem ser abertos em uma sessão ICA. Para obter mais informações, consulte Configurações de política de lista de permissões de canal virtual.

Criando seu próprio canal virtual usando o SDK de Objeto Cliente ICA

Criar um canal virtual usando o Objeto Cliente ICA (ICO) é mais fácil do que usar o SDK de Canal Virtual. Use o ICO criando um objeto nomeado em seu programa usando o método **CreateChannels**.

Importante:

Devido à segurança aprimorada a partir da versão 10.00 do Citrix Receiver para Windows e posterior (e aplicativos Citrix Workspace para Windows), você deve dar um passo extra ao criar um canal virtual ICO.

> Para obter mais informações, consulte Guia do Programador de Especificação da API do Objeto Cliente.

Funcionalidade de passagem de canais virtuais

A maioria dos canais virtuais fornecidos pela Citrix opera sem modificações quando você usa o aplicativo Citrix Workspace para Windows dentro de uma sessão ICA (também conhecida como sessão de passagem). Há considerações ao usar o cliente em saltos extras.

As seguintes funções operam da mesma forma em saltos únicos ou múltiplos:

- Mapeamento de porta COM do cliente
- Mapeamento de unidade do cliente
- Mapeamento de impressora do cliente
- UPD do cliente
- Monitoramento da experiência do usuário final
- USB genérico
- Kerberos
- Suporte multimídia
- Suporte a smartcard
- Passagem transparente de chave
- Twain

Devido à natureza inerente da latência e a fatores como compressão e descompressão e renderização sendo realizados em cada salto, o desempenho pode ser afetado a cada salto adicional que o cliente sofre. As áreas afetadas são:

- Áudio bidirecional
- Transferências de arquivos
- Redirecionamento USB genérico
- Sem interrupções
- Thinwire

> **Importante:**

> Por padrão, as unidades de cliente mapeadas por uma instância do cliente em execução em uma sessão de passagem são restritas às unidades de cliente do cliente de conexão.

Funcionalidade de passagem de canais virtuais entre uma sessão do Citrix Virtual Desktop e uma sessão do Citrix Virtual App

A maioria dos canais virtuais fornecidos pela Citrix opera sem modificações quando você usa o aplicativo Citrix Workspace para Windows dentro de uma sessão ICA em um servidor Citrix Virtual Desktops (também conhecido como sessão de passagem).

Especificamente, no servidor Citrix Virtual Desktops, existe um hook VDA que executa **picaPassthruHook**. Este hook faz com que o cliente pense que está sendo executado em um servidor CPS, colocando o cliente em seu modo de passagem tradicional.

Oferecemos suporte aos seguintes canais virtuais tradicionais e suas funcionalidades:

- Cliente
- Mapeamento de porta COM do cliente
- Mapeamento de unidade do cliente
- Mapeamento de impressora do cliente
- USB genérico (limitado devido ao desempenho)
- Suporte multimídia
- Suporte a smartcard
- SSON
- Passagem transparente de teclas

Segurança e canais virtuais ICA

Garantir a segurança do uso é uma parte importante do planejamento, desenvolvimento e implementação de canais virtuais. Existem várias referências a áreas específicas de segurança localizadas ao longo deste documento.

Práticas recomendadas

Abra os canais virtuais ao **Conectar** e **Reconectar**. Feche os canais virtuais ao fazer logoff e **Desconectar**.

Tenha as seguintes diretrizes em mente ao criar scripts que usam funções de canal virtual.

Nomeando os Canais Virtuais:

Você pode criar um máximo de 32 canais virtuais. Dezessete dos 32 canais são reservados para fins especiais.

- Os nomes dos canais virtuais não devem ter mais de sete caracteres.
- Os três primeiros caracteres são reservados para o nome do fornecedor, e os quatro seguintes para o tipo de canal. Por exemplo, **CTXAUD** representa o canal virtual de áudio da Citrix.

Os canais virtuais são referenciados por um nome ASCII de sete caracteres (ou menos). Em algumas versões anteriores do protocolo ICA, os canais virtuais eram numerados. Os números agora são atribuídos dinamicamente com base no nome ASCII, facilitando a implementação. Usuários que estão desenvolvendo código de canal virtual apenas para uso interno podem usar qualquer nome de sete caracteres que não entre em conflito com os canais virtuais existentes. Use apenas números e ASCII maiúsculas e minúsculas. Siga a convenção de nomenclatura existente ao adicionar seus próprios canais virtuais. Existem vários canais predefinidos. Os canais predefinidos começam com o identificador OEM CTX e são para uso exclusivo da Citrix.

Suporte a Double-Hop:

CANAL VIRTUAL	O DOUBLE HOP É SUPORTADO?
Áudio	Não
Redirecionamento de Conteúdo do Navegador	Não
CDM	Sim
CEIP	Não
Área de Transferência	Sim
Continuum (MRVC)	Não
Control VC	Sim
Redirecionamento de Vídeo HTML5 (v1)	Sim
Teclado, Mouse	Sim
Multitoque	Não

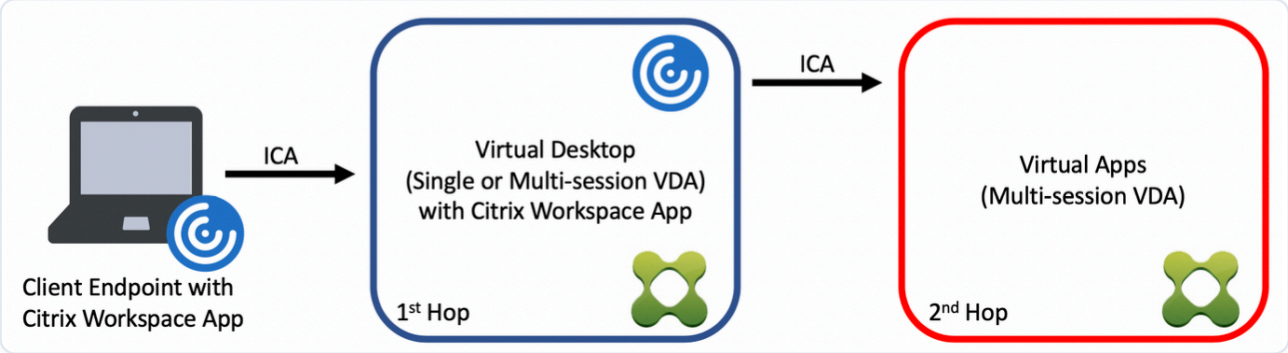
CANAL VIRTUAL	O DOUBLE HOP É SUPORTADO?
NSAPVC	Não
Impressão	Sim
SensVC	Não
Smartcard	Sim
Twain	Sim
USB VC	Sim
Dispositivos WAYCOM -K2M usando VC USB	Sim
Compressão de Vídeo da Webcam	Sim
Redirecionamento de Mídia do Windows	Sim

Consulte também

- SDK de Canal Virtual ICA
- A Citrix Developer Network é o lar de todos os recursos técnicos e discussões envolvendo o uso de SDKs Citrix. Nesta rede, você pode encontrar acesso a SDKs, código de exemplo e scripts, extensões e plug-ins, e documentação de SDK. Também estão incluídos os fóruns da Citrix Developer Network, onde discussões técnicas ocorrem sobre cada um dos SDKs Citrix.

Salto duplo no Citrix DaaS™

No contexto de uma sessão de cliente Citrix, o termo “salto duplo” refere-se a uma sessão do Citrix Virtual App que está sendo executada dentro de uma sessão do Citrix Virtual Desktop. O diagrama a seguir ilustra um salto duplo.



Em um cenário de salto duplo, quando o usuário se conecta a um Citrix Virtual Desktop executado em um VDA de SO de sessão única (conhecido como VDI) ou em um VDA de SO de várias sessões (conhecido como desktop publicado), isso é considerado o primeiro salto. Depois que o usuário se conecta ao desktop virtual, ele pode iniciar uma sessão do Citrix Virtual Apps™. Isso é considerado o segundo salto.

Você pode usar um modelo de implantação de salto duplo para suportar vários casos de uso. O caso em que os ambientes do Citrix Virtual Desktop e do Citrix Virtual Apps são gerenciados por entidades diferentes é um exemplo comum. Esse método também pode ser eficaz na resolução de problemas de compatibilidade de aplicativos.

Requisitos do sistema

Todas as edições do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™) suportam salto duplo.

O primeiro salto deve usar uma versão suportada do VDA de SO de sessão única ou de várias sessões e do Citrix Workspace App. O segundo salto deve usar uma versão suportada do VDA de SO de várias sessões. Consulte a página Matriz de Produtos para ver as versões suportadas.

Para melhor desempenho e compatibilidade, a Citrix recomenda usar um cliente Citrix da mesma versão ou mais recente do que as versões de VDA em uso.

Em ambientes onde o primeiro salto envolve uma solução de desktop virtual de terceiros (não Citrix) em combinação com uma sessão do Citrix Virtual Apps, o suporte é limitado ao ambiente do Citrix Virtual Apps. No caso de quaisquer problemas relacionados ao desktop virtual de terceiros, incluindo - mas não se limitando a - compatibilidade do aplicativo Citrix Workspace™, redirecionamento de dispositivos de hardware e desempenho da sessão, a Citrix pode fornecer suporte técnico com capacidade limitada. Um Citrix Virtual Desktop no primeiro salto pode ser necessário como parte da solução de problemas.

Considerações de implantação para HDX™ em salto duplo

Em geral, cada sessão em um salto duplo é única e as funções cliente-servidor são isoladas para um determinado salto. Esta seção inclui áreas que exigem consideração especial pelos administradores Citrix. A Citrix recomenda que os clientes realizem testes completos dos recursos HDX necessários para garantir que a experiência do usuário e o desempenho sejam adequados para uma determinada configuração de ambiente.

Gráficos

Use as configurações gráficas padrão (codificação seletiva) nos primeiros e segundos saltos. No caso do HDX 3D Pro, a Citrix recomenda fortemente que todos os aplicativos que exigem aceleração gráfica sejam executados localmente no primeiro salto com os recursos de GPU apropriados disponíveis para o VDA.

Latência

A latência de ponta a ponta pode impactar a experiência geral do usuário. Considere a latência adicional entre o primeiro e o segundo salto. Isso é especialmente importante com o redirecionamento de dispositivos de hardware.

Multimídia

A renderização do lado do servidor (na sessão) de conteúdo de áudio e vídeo apresenta o melhor desempenho no primeiro salto. A reprodução de vídeo no segundo salto requer decodificação e recodificação no primeiro salto, aumentando o uso de largura de banda e recursos de hardware como resultado. O conteúdo de áudio e vídeo deve ser limitado ao primeiro salto sempre que possível.

Redirecionamento de dispositivo USB

O HDX inclui modos de redirecionamento genéricos e otimizados para suportar uma ampla gama de tipos de dispositivos USB. Preste atenção especial ao modo em uso em cada salto e use a tabela a seguir como referência para obter os melhores resultados. Para obter mais informações sobre os modos de redirecionamento genéricos e otimizados, consulte Dispositivos USB genéricos.

PRIMEIRO SALTO (VDI OU DESKTOP PUBLICADO)	SEGUNDO SALTO (APLICATIVOS VIRTUAIS)	NOTAS DE SUPORTE
Otimizado	Otimizado	Recomendado (com base no suporte ao dispositivo). Por exemplo, armazenamento em massa USB, scanners TWAIN, webcam, áudio.
Genérico	Genérico	Para dispositivos onde a opção otimizada não está disponível.
Genérico	Otimizado	Embora tecnicamente possível, é recomendado usar o modo otimizado em ambos os saltos quando o suporte ao dispositivo estiver disponível.
Otimizado	Genérico	Não suportado

Nota:

Devido à verbosidade inerente dos protocolos USB, o desempenho pode diminuir entre os saltos. A funcionalidade e os resultados variam dependendo dos requisitos específicos do dispositivo e da aplicação. Testes de validação são altamente recomendados em todos os casos de redirecionamento de dispositivo e especialmente importantes em cenários de duplo salto.

Exceções de suporte

Sessões de salto duplo suportam a maioria dos recursos e capacidades HDX, exceto pelos seguintes:

- Redirecionamento de conteúdo do navegador(/pt-br/citrix-virtual-apps-desktops/multimedia/browser-content-redirection.html)
- Acesso a Aplicativos Locais
- Pacote de Otimização em Tempo Real para Skype for Business
- Otimização para Microsoft Teams(/pt-br/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html)

Conectividade HDX™

O Citrix HDX representa um amplo conjunto de tecnologias que oferecem uma experiência de alta definição aos usuários de aplicativos e desktops centralizados, em qualquer dispositivo e em qualquer rede.

O HDX é projetado com base em três princípios técnicos:

- Redirecionamento inteligente
- Compressão adaptativa
- Desduplicação de dados

Aplicados em diferentes combinações, eles otimizam a experiência de TI e do usuário, diminuem o consumo de largura de banda e aumentam a densidade de usuários por servidor de hospedagem.

Dentro da oferta HDX, você pode se conectar por meio de um protocolo de transporte exclusivo e proprietário, utilizar as unidades máximas de transmissão ao estabelecer sessões e otimizar a conectividade com o Citrix SD-WAN.

Transporte adaptável

O Transporte Adaptável é um mecanismo no Citrix Virtual Apps and Desktops™ que permite estabelecer conexões para sessões HDX usando um protocolo de transporte preferencial, ao mesmo tempo em que oferece um fallback para TCP se a conectividade com o protocolo preferencial estiver indisponível.

Os seguintes protocolos de transporte são suportados:

- Enlightened Data Transport (EDT)
- Transmission Control Protocol (TCP)

Configuração

O Transporte Adaptável é ativado por padrão. Você pode configurar o Transporte Adaptável para operar nos seguintes modos:

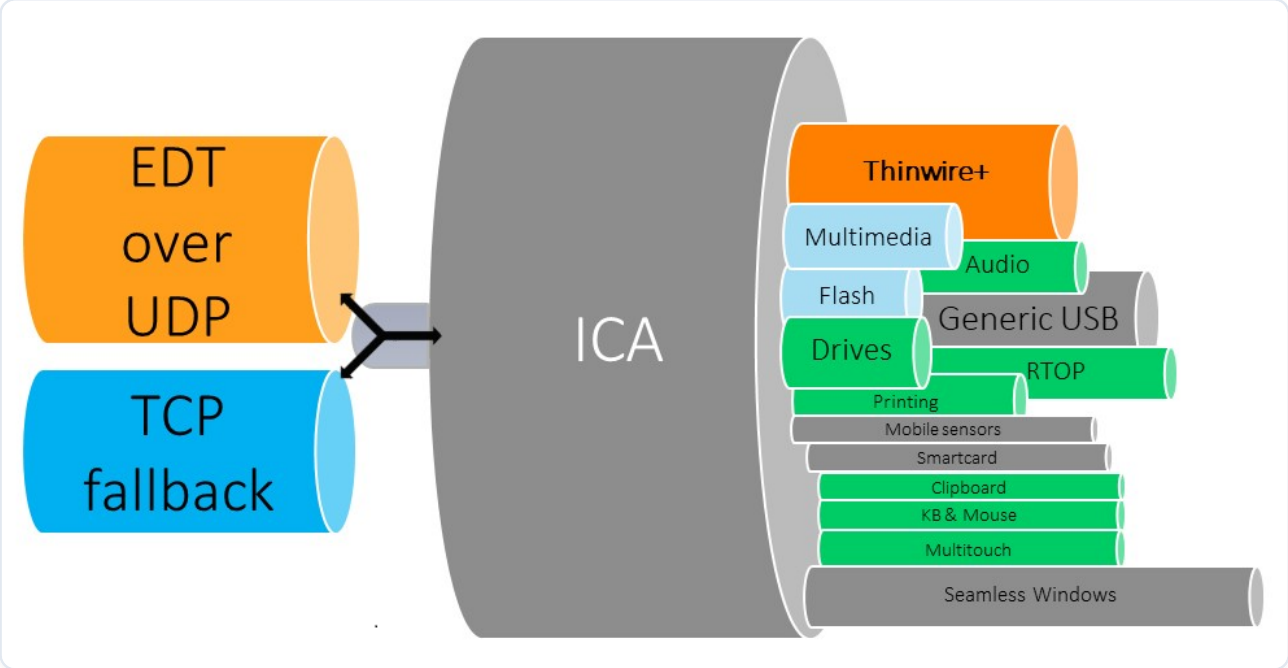
- **Preferencial**: (Padrão) O cliente tenta se conectar com o protocolo preferencial e retorna ao TCP se a conectividade com o protocolo preferencial estiver indisponível.
- **Modo de diagnóstico**: O cliente tenta se conectar apenas usando o protocolo preferencial. O fallback para TCP é desativado.
- **Desativado**: O cliente tenta se conectar apenas usando TCP.

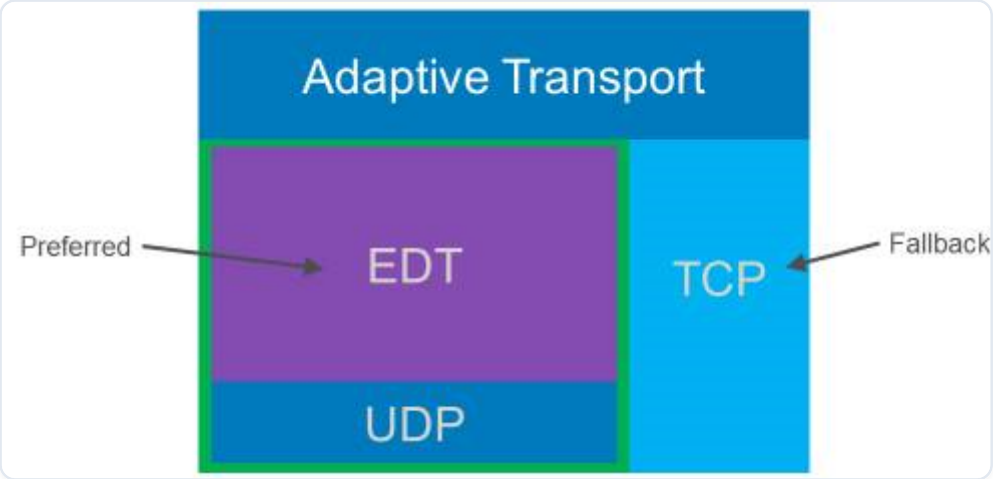
Como funciona

Quando o **Transporte Adaptável** é definido como `Preferred`, o cliente tenta se conectar à sessão com o protocolo preferencial e o TCP em paralelo. Isso permite otimizar o tempo de conexão se não for possível conectar com o protocolo preferencial e o cliente precisar retornar ao uso de TCP. Se a conexão for estabelecida usando TCP, o cliente tenta se conectar com o protocolo preferencial em segundo plano a cada cinco minutos.

Quando o **Transporte Adaptável** é definido como `Diagnostic mode`, o cliente se conecta à sessão apenas com o protocolo preferencial. Se o cliente não conseguir estabelecer uma conexão usando o protocolo preferencial, ele não retorna ao uso de TCP e a conexão falha.

Quando o **Transporte Adaptável** é definido como `Off`, o **Transporte Adaptável** é desativado e o cliente se conecta à sessão usando apenas TCP.





Requisitos do sistema

A seguir estão os requisitos para usar o Transporte Adaptável e o EDT:

- Plano de controle
  - Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops service)
  - Citrix Virtual Apps and Desktops: versão atualmente suportada
- Virtual Delivery Agent
  - Windows: versão atualmente suportada (2402 ou posterior recomendado)
  - Linux: versão atualmente suportada (2402 ou posterior recomendado)
- Aplicativo Citrix Workspace™
  - Windows: versão atualmente suportada (2402 ou posterior recomendado)
  - Linux: versão atualmente suportada (2402 ou posterior recomendado)
  - Mac: versão atualmente suportada (2402 ou posterior recomendado)
  - iOS: versão mais recente disponível na Apple App Store
  - Android: versão mais recente disponível no Google Play
- Citrix NetScaler® Gateway
  - 14.1.12.30 ou posterior (recomendado)
  - 13.1.17.42 ou posterior (13.1-52.19 ou posterior recomendado)

> **Nota:**

> Para obter detalhes sobre o Linux VDA, consulte a documentação do Linux Virtual Delivery Agent.

Requisitos de rede

As seções a seguir são os requisitos de rede para usar o EDT com o Adaptive Transport:

Hosts de sessão

Se seus hosts de sessão tiverem um firewall, como o Firewall do Windows Defender, você deve permitir o seguinte tráfego de entrada para conexões internas.

DESCRIÇÃO	ORIGEM	PROTOCOLO	PORTA
Conexão interna - Confiabilidade da sessão ativada	Cliente	UDP	2598
Conexão interna - Confiabilidade da Sessão desativada			1494
Conexão interna - HDX™ Direct ou VDA SSL			443

> **Nota:**

> O instalador do VDA adiciona as regras de entrada apropriadas ao Firewall do Windows Defender. Se você usar um firewall diferente, deverá adicionar as regras acima.

Rede interna

A tabela a seguir descreve as regras de firewall necessárias para usar o EDT em sua rede:

DESCRIÇÃO	PROTOCOLO	ORIGEM	DESTINO	PORTA DE DESTINO
Conexão interna direta - Confiabilidade	UDP	Rede do cliente	Rede VDA	2598

DESCRIÇÃO	PROTOCOLO	ORIGEM	DESTINO	PORTA DE DESTINO
da Sessão ativada				
Conexão interna direta - Confiabilidade da Sessão desativada				1494
Conexão interna direta - HDX Direto ou VDA SSL				443
NetScaler Gateway		NetScaler SNIP		2598
NetScaler Gateway - VDA SSL				443

Nota:

Se você estiver usando o Citrix Gateway Service, você deve habilitar **Rendezvous** para usar EDT como seu protocolo de transporte. Consulte a documentação Rendezvous para requisitos de sistema e rede.

Rede do cliente

A tabela a seguir descreve os requisitos de conectividade para dispositivos cliente:

DESCRIÇÃO	PROTOCOLO	ORIGEM	DESTINO	PORTA DE DESTINO
Conexão interna - Confiabilidade	UDP	IP do cliente	Rede VDA	2598

DESCRIÇÃO	PROTOCOLO	ORIGEM	DESTINO	PORTA DE DESTINO
da sessão habilitada				
Conexão interna - Confiabilidade da sessão desabilitada				1494
Conexão interna - HDX Direct ou SSL VDA				443
Conexão externa - NetScaler Gateway			Endereço IP público do NetScaler Gateway	443
Conexão externa - Citrix Gateway Service			Citrix Gateway Service	443

Nota:

Se você estiver usando o Citrix Gateway Service, os clientes devem ser capazes de acessar `<https://*.*.nssvc.net>`. Se você não puder permitir todos os subdomínios usando `<https://*.*.nssvc.net>`, você pode usar `<https://*.c.nssvc.net>` e `<https://*.g.nssvc.net>` em vez disso. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX270584.

Enlightened Data Transport

Enlightened Data Transport (EDT) é um protocolo de transporte proprietário da Citrix construído sobre o User Datagram Protocol (UDP). Ele oferece uma experiência de usuário superior em conexões de longa distância desafiadoras, mantendo a escalabilidade do servidor. O EDT melhora

o throughput de dados para todos os canais virtuais ICA® em redes não confiáveis, proporcionando uma experiência de usuário melhor e mais consistente.

Quando o **Transporte Adaptável** está habilitado, o EDT é o protocolo preferencial.

Coisas a saber

- A **Confiabilidade da Sessão** deve estar habilitada para usar a **Descoberta de MTU** e o EDT com o NetScaler® Gateway e o Citrix Gateway Service.
- A fragmentação de pacotes pode causar degradação do desempenho ou até mesmo falha na abertura de sessões em alguns casos. Para evitar isso, você deve ajustar o MTU do EDT para um valor adequado às suas redes. Você pode usar a Descoberta de MTU do EDT ou uma solução alternativa manual descrita em Como configurar o MSS ao usar o EDT em redes com MTU não padrão.
- Para obter detalhes sobre como habilitar o uso do EDT com o NetScaler Gateway, consulte Configurar o NetScaler Gateway para oferecer suporte ao Enlightened Data Transport.

Descoberta de MTU do EDT

A Descoberta de MTU permite que o EDT determine automaticamente a Unidade Máxima de Transmissão (MTU) ao estabelecer uma sessão. Isso evita a fragmentação de pacotes EDT que pode resultar em degradação do desempenho ou falha no estabelecimento de uma sessão.

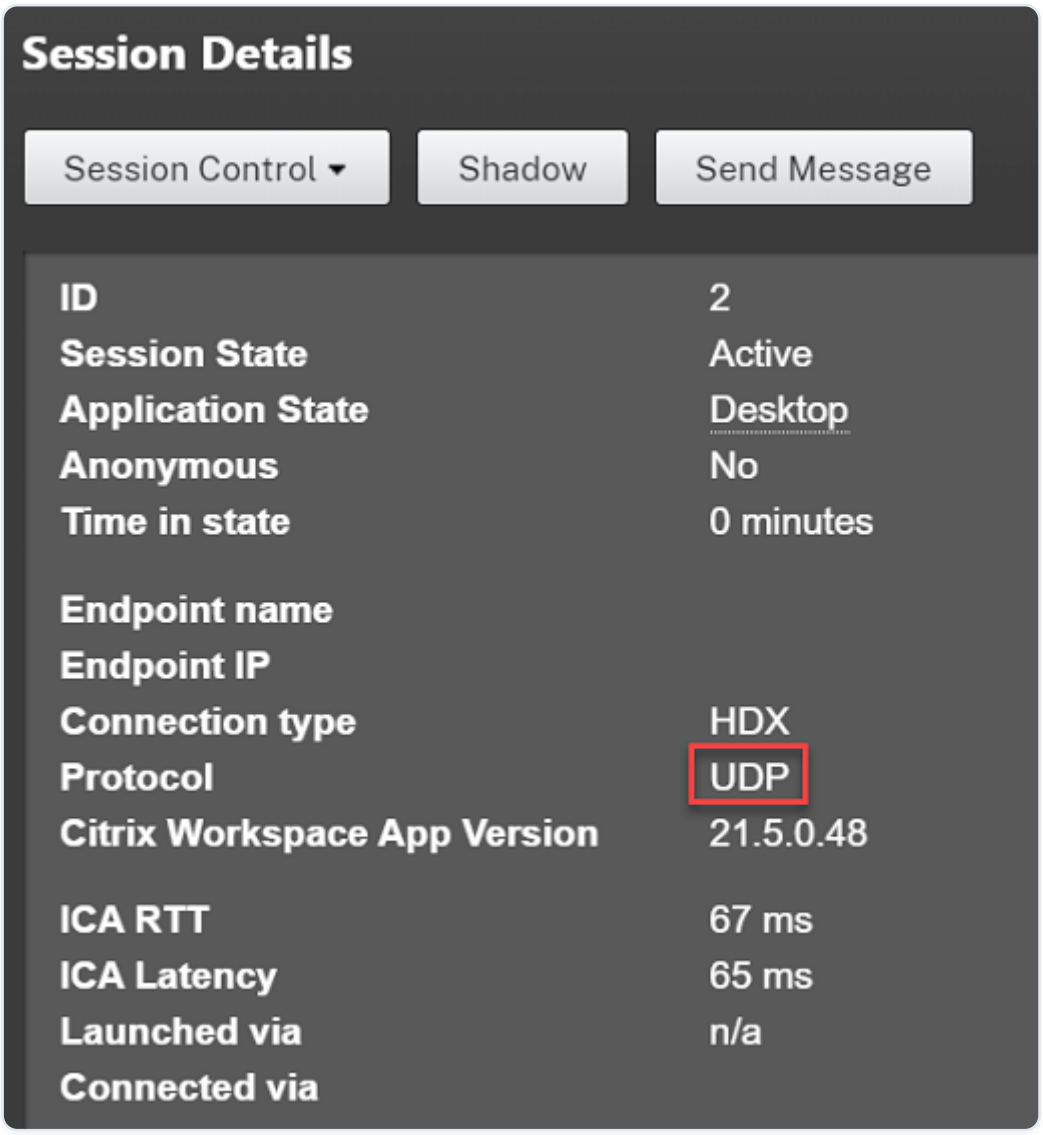
A Descoberta de MTU está habilitada por padrão. Se você precisar desabilitá-la, consulte Recursos HDX gerenciados através do registro para obter detalhes.

> **Nota:**
>
> - A **Confiabilidade da Sessão** deve estar habilitada para que a Descoberta de MTU funcione.
> - A Descoberta de MTU com Multi-Stream ICA está disponível com as versões VDA 2209 e posteriores.

Solução de problemas

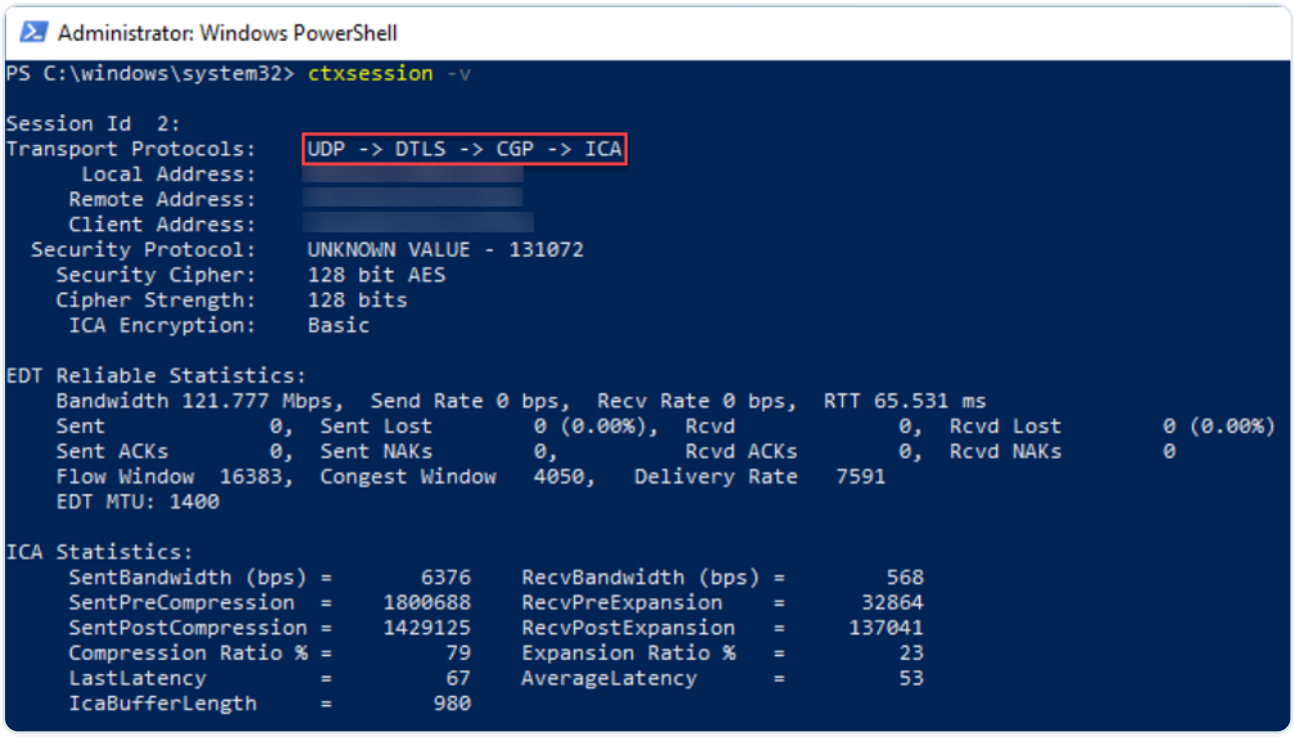
Para confirmar que o EDT está sendo usado como protocolo de transporte para a sessão, você pode usar o Director ou o utilitário de linha de comando `CtxSession.exe` no VDA.

No Director, procure a sessão e selecione **Detalhes**. Se o **Tipo de conexão** for `HDX` e o **Protocolo** for `UDP`, o EDT estará sendo usado como protocolo de transporte para a sessão.



Para usar o utilitário CtxSession.exe, inicie um Prompt de Comando ou PowerShell dentro da sessão e execute `ctxsession.exe`. Para ver estatísticas detalhadas, execute `ctxsession.exe -v`. Se o EDT estiver em uso, o protocolo de transporte mostrará um dos seguintes:

- **UDP > ICA®** (Confiabilidade da sessão desabilitada)
- **UDP > CGP > ICA** (Confiabilidade da sessão habilitada)
- **UDP > DTLS > CGP > ICA** (ICA é criptografado de ponta a ponta com DTLS)



Quando as sessões falham ao conectar com EDT

Para solucionar problemas de **Transporte Adaptável** e **EDT**, sugerimos o seguinte:

1. Revise os Requisitos do sistema, Requisitos de rede, Problemas conhecidos e Coisas a saber, e certifique-se de que todos os itens foram abordados.
2. Verifique se há políticas Citrix® no Studio ou GPO substituindo a configuração desejada de **Transporte Adaptável HDX**.
3. Verifique se há configurações no cliente substituindo a configuração desejada de Transporte Adaptável HDX. Isso pode ser uma preferência de GPO, uma configuração usando o modelo administrativo opcional do aplicativo Workspace ou uma configuração manual da configuração **HDXoverUDP** no registro ou no arquivo de configuração do cliente.
4. Em máquinas VDA de várias sessões, certifique-se de que os ouvintes UDP estejam ativos. Abra um prompt de comando na máquina VDA e execute `netstat -a -p udp`. Para obter mais informações, consulte Como confirmar o protocolo de transporte de dados iluminado HDX.
5. Verifique se as regras de firewall apropriadas foram configuradas tanto nos firewalls de rede quanto nos firewalls em execução nas máquinas VDA.
6. Inicie uma sessão direta internamente, ignorando o NetScaler® Gateway ou o Citrix Gateway Service, e verifique o protocolo em uso. Se a sessão usar EDT, o VDA estará pronto para usar EDT para conexões externas através do NetScaler Gateway ou do Citrix Gateway Service.

7. Se o EDT funcionar para conexões internas diretas e não para sessões que passam pelo NetScaler Gateway ou Citrix Gateway Service:
    - Certifique-se de que a **Confiabilidade da Sessão** esteja ativada.
    - Se estiver usando o NetScaler Gateway, certifique-se de que sua configuração esteja de acordo com a configuração necessária descrita em Configurar o NetScaler Gateway para oferecer suporte ao Enlightened Data Transport e ao HDX Insight.
8. Se estiver usando o Citrix Gateway Service, certifique-se de que o Rendezvous esteja ativado e funcionando.
9. Verifique se as conexões dos seus usuários exigem um MTU não padrão. Conexões com um MTU efetivo inferior a 1500 bytes causam fragmentação de pacotes EDT, o que, por sua vez, pode afetar o desempenho ou até mesmo causar falhas no lançamento da sessão. Esse problema é comum ao usar VPNs, alguns pontos de acesso Wi-Fi e redes móveis, como 4G e 5G. Certifique-se de ter a Descoberta de MTU ativada ou de estar configurando um MTU personalizado conforme descrito em Como configurar o MSS ao usar EDT em redes com MTU não padrão.

Problemas conhecidos

- Caminhos de rede assimétricos podem fazer com que a Descoberta de MTU falhe para conexões que não passam pelo NetScaler Gateway ou Citrix Gateway Service. Para resolver esse problema, atualize para a versão 2103 ou posterior do VDA.
- Ao usar o NetScaler Gateway, caminhos de rede assimétricos podem fazer com que a Descoberta de MTU falhe. Isso ocorre devido a um problema no Gateway que faz com que o bit Don’t Fragment (DF) no cabeçalho dos pacotes EDT não seja propagado. Uma correção para esse problema está disponível, a partir da versão de firmware 13.1 build 17.42. Para obter detalhes sobre como ativar a correção, consulte a documentação do NetScaler Gateway.
- A Descoberta de MTU pode falhar para usuários que se conectam por meio de uma rede DS-Lite. Alguns modems não respeitam o bit DF quando o processamento de pacotes está ativado, impedindo que a Descoberta de MTU detecte a fragmentação. Nesta situação, as seguintes opções estão disponíveis:
    - Desative o processamento de pacotes no modem do usuário.
    - Desative a **Descoberta de MTU** e use um MTU codificado, conforme descrito em Como configurar o MSS ao usar EDT em redes com MTU não padrão.

- Desative o **Transporte Adaptável** para forçar as sessões a usar TCP. Se apenas um subconjunto de usuários for afetado, considere desativá-lo no lado do cliente para que outros usuários possam continuar a usar o EDT.

Protocolo Rendezvous

Ao usar o Citrix Gateway Service, o protocolo Rendezvous permite que os VDAs ignorem os Citrix Cloud™ Connectors para se conectar direta e seguramente com o plano de controle do Citrix Cloud.

Existem dois tipos de tráfego a serem considerados:

1. Tráfego de controle para registro de VDA e intermediação de sessão.
2. Tráfego de sessão HDX™.

Existem duas versões do Rendezvous disponíveis:

- Versão 1 (V1): suporta ignorar os Citrix Cloud Connectors apenas para tráfego de sessão HDX.
- Versão 2 (V2): suporta ignorar os Citrix Cloud Connectors tanto para tráfego de controle quanto para tráfego de sessão HDX.

Para detalhes sobre requisitos de sistema, considerações e configuração para cada uma das versões do Rendezvous, revise a documentação respectiva.

Documentação do Rendezvous V1

Documentação do Rendezvous V2

Rendezvous V1

Ao usar o Citrix Gateway Service, o protocolo Rendezvous permite que os VDAs ignorem os Citrix Cloud™ Connectors para se conectar direta e seguramente com o plano de controle do Citrix Cloud.

Requisitos

- Acesso ao ambiente usando Citrix® StoreFront Cloud e Citrix Gateway service.
- Plano de Controle: Citrix DaaS™ (Citrix Cloud).
- VDA: Versão 1912 ou posterior.
  - A versão 2012 é a mínima exigida para o EDT Rendezvous.

  - A versão 2012 é a mínima exigida para suporte a proxy não transparente (sem suporte a arquivo PAC).
  - A versão 2103 é a mínima exigida para configuração de proxy com um arquivo PAC.

- Habilite o protocolo Rendezvous na política Citrix. Para mais informações, consulte Configuração da política do protocolo Rendezvous.
- Os VDAs devem ter acesso a `https://*.nssvc.net`, incluindo todos os subdomínios. Se você não conseguir adicionar todos os subdomínios à lista de permissões dessa forma, use `https://*.c.nssvc.net` e `https://*.g.nssvc.net`. Para mais informações, consulte a seção Requisitos de Conectividade com a Internet da documentação do Citrix Cloud (em Citrix DaaS) e o artigo da Central de Conhecimento CTX270584.
- Os VDAs devem ser capazes de se conectar aos endereços mencionados anteriormente nas portas TCP 443 e UDP 443 para TCP Rendezvous e EDT Rendezvous, respectivamente.
- Os Cloud Connectors devem obter os FQDNs dos VDAs ao intermediar uma sessão. Realize esta tarefa de uma destas duas maneiras:

  - **Habilitar resolução de DNS para o site.** navegar até **Configurações > Configurações do site** e ative a configuração **Habilitar resolução de DNS**. Alternativamente, use o Citrix Virtual Apps and Desktops Remote PowerShell SDK e execute o comando `Set-BrokerSite -DnsResolutionEnabled $true`. Para mais informações sobre o Citrix Virtual Apps and Desktops Remote PowerShell SDK, consulte SDKs e APIs.
  - **Zona de pesquisa inversa de DNS com registros PTR para os VDAs.** Se você escolher esta opção, recomendamos que você configure os VDAs para sempre tentar registrar registros PTR. Para fazer isso, use o Editor de Política de Grupo ou Objeto de Política de Grupo, navegar até **Configuração do Computador > Modelos Administrativos > Rede > Cliente DNS**, e defina **Registrar Registros PTR** como **Habilitado e Registrar**. Se o sufixo DNS da conexão não corresponder ao sufixo DNS do domínio, você também deve configurar a configuração **Sufixo DNS específico da conexão** para que as máquinas registrem os registros PTR com sucesso.

> **Nota:**
>
> Se estiver usando a opção de resolução de DNS, os Cloud Connectors devem ser capazes de resolver os nomes de domínio totalmente qualificados (FQDNs) das máquinas VDA. No caso de usuários internos se conectarem diretamente às máquinas

> VDA, os dispositivos cliente também devem ser capazes de resolver os FQDNs das máquinas VDA.

> Se estiver usando uma zona de pesquisa inversa de DNS, os FQDNs nos registros PTR devem corresponder aos FQDNs das máquinas VDA. Se o registro PTR contiver um FQDN diferente, a conexão Rendezvous falhará. Por exemplo, se o FQDN da máquina for `vda01.domain.net`, o registro PTR deve conter `vda01.domain.net`. Um FQDN diferente, como `vda01.sub.domain.net`, não funcionará.

Configuração de proxy

O VDA oferece suporte ao estabelecimento de conexões Rendezvous por meio de um proxy.

Considerações sobre proxy

Considere o seguinte ao usar proxies com o Rendezvous:

- Proxies transparentes, proxies HTTP não transparentes e proxies SOCKS5 são suportados.
- A descriptografia e inspeção de pacotes não são suportadas. Configure uma exceção para que o tráfego ICA® entre o VDA e o Gateway Service não seja interceptado, descriptografado ou inspecionado. Caso contrário, a conexão será interrompida.
- Proxies HTTP suportam autenticação baseada em máquina usando os protocolos de autenticação Negotiate e Kerberos ou NT LAN Manager (NTLM).

  Ao se conectar ao servidor proxy, o esquema de autenticação Negotiate seleciona automaticamente o protocolo Kerberos. Se o Kerberos não for suportado, o Negotiate retorna ao NTLM para autenticação.

> **Nota:**

> Para usar o Kerberos, você deve criar o nome principal de serviço (SPN) para o servidor proxy e associá-lo à conta do Active Directory do proxy. O VDA gera o SPN no formato `HTTP/<proxyURL>` ao estabelecer uma sessão, onde a URL do proxy é recuperada da configuração da política de **proxy Rendezvous**. Se você não criar um SPN, a autenticação retornará ao NTLM. Em ambos os casos, a identidade da máquina VDA é usada para autenticação.

- A autenticação com um proxy SOCKS5 não é atualmente suportada. Se estiver usando um proxy SOCKS5, você deve configurar uma exceção para que o tráfego destinado aos endereços do Gateway Service (especificados nos requisitos) possa ignorar a autenticação.
- Apenas proxies SOCKS5 suportam transporte de dados via EDT. Para um proxy HTTP, use TCP como protocolo de transporte para ICA.

Proxy transparente

Se estiver usando um proxy transparente em sua rede, nenhuma configuração adicional é necessária no VDA.

Proxy não transparente

Se estiver usando um proxy não transparente em sua rede, configure a configuração Rendezvous proxy configuration. Quando a configuração estiver habilitada, especifique o endereço do proxy HTTP ou SOCKS5, ou insira o caminho para o arquivo PAC para que o VDA saiba qual proxy usar. Por exemplo:

- Endereço do proxy: `http://<URL or IP>:<port>` ou `socks5://<URL or IP>:<port>`
- Arquivo PAC: `http://<URL or IP>/<path>/<filename>.pac`

Se você usar o arquivo PAC para configurar o proxy, defina o proxy usando a sintaxe exigida pelo serviço HTTP do Windows: `PROXY [<scheme>=]<URL or IP>:<port>`. Por exemplo, `PROXY socks5=<URL or IP>:<port>`.

Validação do Rendezvous

Se você atender a todos os requisitos, siga estas etapas para validar se o Rendezvous está em uso:

1. Inicie o PowerShell ou um prompt de comando dentro da sessão HDX™.
2. Execute `ctxsession.exe –v`.
3. Os protocolos de transporte em uso indicam o tipo de conexão:
    - Rendezvous TCP: **TCP > SSL > CGP > ICA**
    - Rendezvous EDT: **UDP > DTLS > CGP > ICA**
    - Proxy via Cloud Connector: **TCP > CGP > ICA**

Outras considerações

Ordem do conjunto de cifras do Windows

Para uma ordem de conjunto de cifras personalizada, certifique-se de incluir os conjuntos de cifras suportados pelo VDA da seguinte lista:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Se a ordem do conjunto de cifras personalizada não contiver esses conjuntos de cifras, a conexão Rendezvous falhará.

Acesso Privado Zscaler

Se estiver usando o Zscaler Private Access (ZPA), é recomendável que você configure as configurações de bypass para o Serviço de Gateway para evitar o aumento da latência e o impacto no desempenho associado. Para fazer isso, você deve definir segmentos de aplicativo para os endereços do Serviço de Gateway – especificados nos requisitos – e configurá-los para sempre ignorar. Para obter informações sobre como configurar segmentos de aplicativo para ignorar o ZPA, consulte a documentação do Zscaler.

Rendezvous V2

Ao usar o Citrix Gateway Service, o protocolo Rendezvous permite que os VDAs ignorem os Citrix Cloud™ Connectors para se conectar direta e seguramente com o plano de controle do Citrix Cloud.

O Rendezvous V2 é compatível com máquinas padrão ingressadas no domínio, máquinas ingressadas no Microsoft Entra híbrido, máquinas ingressadas no Microsoft Entra e máquinas não ingressadas no domínio.

> **Nota:**
>
> Atualmente, implantações sem conector são possíveis apenas com máquinas *ingressadas no Azure AD* e *não ingressadas no domínio*. Máquinas padrão ingressadas no domínio AD e máquinas ingressadas no Microsoft Entra híbrido ainda exigem Cloud Connectors para registro de VDA e intermediação de sessão. No entanto, não há requisitos de DNS para usar o Rendezvous V2.

> Os requisitos do Cloud Connector para outras funções não relacionadas à comunicação do VDA, como conectar-se ao seu domínio AD local, provisionamento MCS para hipervisores locais, etc., permanecem os mesmos.

Requisitos

Os requisitos para usar o Rendezvous V2 são:

- Acesso ao ambiente usando Citrix® StoreFront Cloud e Citrix Gateway Service
- Plano de controle: Citrix DaaS™
- Versão do VDA 2203
- Habilite o protocolo Rendezvous na política Citrix. Para obter mais informações, consulte Configuração da política do protocolo Rendezvous.
- A Confiabilidade da Sessão deve estar habilitada nos VDAs
- As máquinas VDA devem ter acesso a:
  - `https://*.xendesktop.net` em `TCP 443`. Se você não puder permitir todos os subdomínios dessa maneira, poderá usar `https://<customer_ID>.xendesktop.net`, onde \<customer_ID\> é o seu ID de cliente do Citrix Cloud, conforme mostrado no portal do administrador do Citrix Cloud.
  - `https://*.*.nssvc.net` em `TCP 443` para a conexão de controle com o Serviço Gateway.
  - `https://*.*.nssvc.net` em `TCP 443` e `UDP 443` para sessões HDX via TCP e EDT, respectivamente.

> **Nota:**
>
> Se você não puder permitir todos os subdomínios usando `https://*.*.nssvc.net`, você pode usar `https://*.c.nssvc.net` e `https://*.g.nssvc.net` em vez disso. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX270584.

Configuração de proxy

O VDA oferece suporte à conexão por meio de proxies para tráfego de controle e tráfego de sessão HDX™ ao usar o Rendezvous. Os requisitos e considerações para ambos os tipos de tráfego são diferentes, portanto, revise-os cuidadosamente.

Considerações sobre proxy de tráfego de controle

- Somente proxies HTTP são suportados.
- A descriptografia e inspeção de pacotes não são suportadas. Configure uma exceção para que o tráfego de controle entre o VDA e o plano de controle do Citrix Cloud não seja interceptado, descriptografado ou inspecionado. Caso contrário, a conexão falha.
- A autenticação baseada em máquina é suportada apenas se a máquina VDA estiver ingressada no domínio AD. Ela pode usar autenticação Negotiate/Kerberos ou NTLM.

> **Nota:**
>
> Para usar o Kerberos, crie o nome principal de serviço (SPN) para o servidor proxy e associe-o à conta do Active Directory do proxy. O VDA gera o SPN no formato `HTTP/<proxyURL>` ao estabelecer uma conexão com o Citrix Cloud. Se você não criar um SPN, a autenticação retornará ao NTLM. Em ambos os casos, a identidade da máquina VDA é usada para autenticação.

Considerações sobre proxy de tráfego HDX

- Proxies HTTP e SOCKS5 são suportados.
- O EDT só pode ser usado com proxies SOCKS5.
- Por padrão, o tráfego HDX usa o proxy definido para o tráfego de controle. Se você precisar usar um proxy diferente para o tráfego HDX, seja um proxy HTTP diferente ou um proxy SOCKS5, use a configuração de política Rendezvous proxy configuration.
- A descriptografia e inspeção de pacotes não são suportadas. Configure uma exceção para que o tráfego HDX entre o VDA e o plano de controle do Citrix Cloud não seja interceptado, descriptografado ou inspecionado. Caso contrário, a conexão falhará.
- A autenticação baseada em máquina é suportada apenas com proxies HTTP e se a máquina VDA estiver ingressada no domínio AD. Ela pode usar autenticação Negotiate/Kerberos ou NTLM.

> **Nota:**
>
> Para usar o Kerberos, crie o nome principal de serviço (SPN) para o servidor proxy e associe-o à conta do Active Directory do proxy. O VDA gera o SPN no formato `HTTP/<proxyURL>` ao estabelecer uma sessão, onde a URL do proxy é recuperada da

> configuração de política Rendezvous proxy configuration. Se você não criar um SPN, a autenticação retornará ao NTLM. Em ambos os casos, a identidade da máquina VDA é usada para autenticação.

- A autenticação com um proxy SOCKS5 não é atualmente suportada. Se estiver usando um proxy SOCKS5, configure uma exceção para que o tráfego destinado aos endereços do Gateway Service (especificados nos requisitos) possa ignorar a autenticação.
- Apenas proxies SOCKS5 suportam transporte de dados via EDT. Para um proxy HTTP, use TCP como protocolo de transporte para ICA.

Proxy transparente

Se estiver usando um proxy transparente em sua rede, nenhuma configuração adicional é necessária no VDA.

Proxy não transparente

Se estiver usando um proxy não transparente em sua rede, especifique o proxy durante a instalação do VDA para que o tráfego de controle possa alcançar o plano de controle do Citrix Cloud. Certifique-se de revisar as considerações do proxy de tráfego de controle antes de prosseguir com a instalação e configuração.

No assistente de instalação do VDA, selecione **Rendezvous Proxy Configuration** na página **Additional Components**. Esta opção torna a página **Rendezvous Proxy Configuration** disponível posteriormente no assistente de instalação. Uma vez aqui, insira o endereço do proxy ou o caminho para o arquivo PAC para que o VDA saiba qual proxy usar. Por exemplo:

- Endereço do proxy: `http://<URL or IP>:<port>`
- Arquivo PAC: `http://<URL or IP>/<path/<filename>.pac`

Conforme declarado nas considerações do proxy de tráfego HDX, o tráfego HDX usa o proxy definido durante a instalação do VDA por padrão. Se você precisar usar um proxy diferente para o tráfego HDX, seja um proxy HTTP diferente ou um proxy SOCKS5, use a configuração de política Rendezvous proxy configuration. Quando a configuração estiver habilitada, especifique o endereço do proxy HTTP ou SOCKS5. Você também pode inserir o caminho para o arquivo PAC para que o VDA saiba qual proxy usar. Por exemplo:

- Endereço do proxy: `http://<URL or IP>:<port>` ou `socks5://<URL or IP>:<port>`
- Arquivo PAC: `http://<URL or IP>/<path/<filename>.pac`

Se você usar o arquivo PAC para configurar o proxy, defina o proxy usando a sintaxe exigida pelo serviço HTTP do Windows: `PROXY [<scheme>=]<URL or IP>:<port>`. Por exemplo, `PROXY socks5=<URL or IP>:<port>.`.

Como configurar o Rendezvous

A seguir estão as etapas para configurar o Rendezvous em seu ambiente:

1. Certifique-se de que todos os requisitos sejam atendidos.
2. Se você precisar usar um proxy HTTP não transparente em seu ambiente, configure-o durante a instalação do VDA. Consulte a seção configuração do proxy para obter detalhes.
3. Reinicie a máquina VDA após a conclusão da instalação.
4. Crie uma política Citrix ou edite uma existente:
    - Defina a configuração **Protocolo Rendezvous** como **Permitido**.
    - Se você precisar configurar um proxy HTTP ou SOCKS5 para tráfego HDX, configure a configuração **Configuração de proxy do Rendezvous**.
    - Certifique-se de que os filtros da política Citrix estejam configurados corretamente. A política se aplica às máquinas que precisam ter o Rendezvous ativado.
5. Certifique-se de que a política Citrix tenha a prioridade correta para que não sobrescreva outra.

> **Observação:**
>
> Se você estiver usando o VDA versão 2308 ou anterior, o V1 é usado por padrão. Para obter mais informações sobre como configurar a versão a ser usada, consulte Recursos HDX gerenciados por meio do registro.

Validação do Rendezvous

Se você atende a todos os requisitos e concluiu a configuração, siga estas etapas para validar se o Rendezvous está em uso:

1. Dentro do desktop virtual, abra um prompt de comando ou PowerShell.
2. Execute `ctxsession.exe -v`.
3. Os protocolos de transporte exibidos indicam o tipo de conexão:
    - Rendezvous TCP: TCP > SSL > CGP > ICA

- Rendezvous EDT: UDP > DTLS > CGP > ICA
- Não é Rendezvous: TCP > CGP > ICA

4. A versão do Rendezvous relatada indica a versão em uso.

Outras considerações

Ordem da suíte de cifras do Windows

Se a ordem da suíte de cifras foi modificada nas máquinas VDA, certifique-se de incluir as suítes de cifras suportadas pelo VDA:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Se a ordem personalizada do conjunto de cifras não contiver esses conjuntos de cifras, a conexão Rendezvous falhará.

Acesso Privado Zscaler

Se estiver usando o Zscaler Private Access (ZPA), é recomendável configurar as configurações de bypass para o Serviço de Gateway para evitar o aumento da latência e o impacto no desempenho associado. Para fazer isso, você deve definir segmentos de aplicativo para os endereços do Serviço de Gateway – especificados nos requisitos – e configurá-los para sempre ignorar. Para obter informações sobre como configurar segmentos de aplicativo para ignorar o ZPA, consulte a documentação do Zscaler.

Problemas Conhecidos

O instalador do VDA 2203 não permite inserir uma barra (/) para o endereço do proxy

Como solução alternativa, você pode configurar o proxy no registro após a instalação do VDA:

```
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent

Value type: String

Value name: ProxySettings

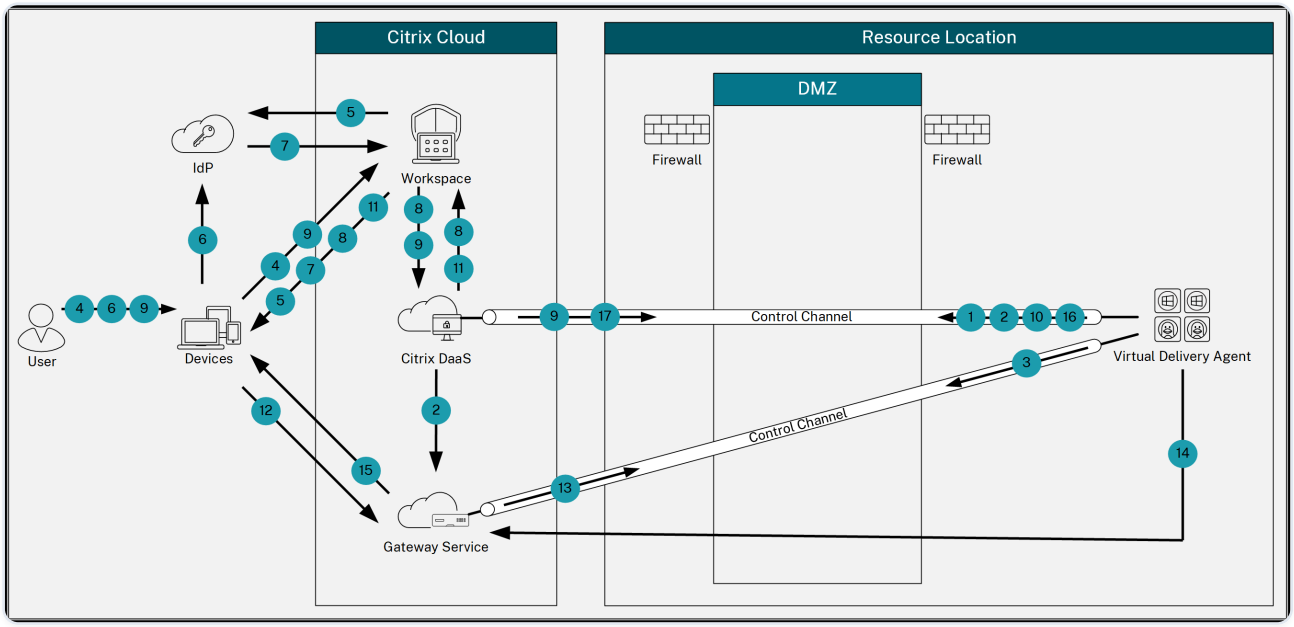
Value data: Proxy address or path to pac file. For example:

    Proxy address: http://squidk.test.local:3128
```

```
Pac file: http://file.test.com/config/proxy.pac
```

Fluxo de tráfego Rendezvous

O diagrama a seguir ilustra a sequência de etapas sobre o fluxo de tráfego Rendezvous.



1. O VDA estabelece uma conexão WebSocket com o Citrix Cloud e se registra.
2. O VDA se registra no Serviço de Gateway Citrix e obtém um token dedicado.
3. O VDA estabelece uma conexão de controle persistente com o Serviço de Gateway.
4. O usuário navega até o URL da sua loja.
5. O Citrix® StoreFront Cloud avalia a configuração de autenticação e redireciona os usuários para o IdP apropriado para autenticação.
6. O usuário insere suas credenciais.
7. Após validar com sucesso as credenciais do usuário, o usuário é redirecionado para o Citrix® StoreFront Cloud.
8. O Citrix® StoreFront Cloud contabiliza os recursos para o usuário e os exibe.
9. O usuário seleciona um desktop ou aplicativo da loja. O Citrix® StoreFront Cloud envia a solicitação ao Citrix DaaS, que intermedia a conexão e instrui o VDA a se preparar para a sessão.
10. O VDA responde com a capacidade Rendezvous e sua identidade.
11. O Citrix DaaS gera um tíquete de inicialização e o envia para o dispositivo do usuário através do Citrix® StoreFront Cloud.

12. O endpoint do usuário se conecta ao Gateway Service e fornece o tíquete de inicialização para autenticar e identificar o recurso ao qual se conectar.
13. O Gateway Service envia as informações de conexão para o VDA.
14. O VDA estabelece uma conexão direta para a sessão com o Gateway Service.
15. O Gateway Service completa a conexão entre o endpoint e o VDA.
16. O VDA verifica o licenciamento para a sessão.
17. O Citrix DaaS envia as políticas aplicáveis para o VDA.

HDX™ Direct

Ao acessar recursos fornecidos pela Citrix, o HDX Direct permite que dispositivos cliente internos e externos estabeleçam uma conexão direta segura com o host da sessão, se a comunicação direta for possível.

Requisitos do sistema

A seguir estão os requisitos do sistema para usar o HDX Direct:

- Plano de controle
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops™ 2503 ou posterior
- Virtual Delivery Agent (VDA)
  - Windows: versão 2503 ou posterior
- Aplicativo Workspace
  - Windows: versão 2503 ou posterior
  - Linux: versão 2411 ou posterior
  - Mac: versão 2411 ou posterior
- Camada de acesso
  - Citrix® StoreFront Cloud
  - Citrix StoreFront 2503 ou posterior
  - Citrix Gateway Service
  - Citrix NetScaler® Gateway

Requisitos de rede

A seguir estão os requisitos de rede para usar o HDX Direct.

Hosts de sessão

Se seus hosts de sessão tiverem um firewall, como o Firewall do Windows Defender, você deve permitir o seguinte tráfego de entrada para conexões internas.

DESCRIÇÃO	ORIGEM	PROTOCOLO	PORTA
Conexão interna direta	Cliente	TCP	443
Conexão interna direta	Cliente	UDP	443

> Nota:
>
> O instalador do VDA adiciona as regras de entrada apropriadas ao Firewall do Windows Defender. Se você usar um firewall diferente, deverá adicionar as regras acima.

Rede do cliente

A tabela a seguir descreve a rede do cliente para usuários internos e externos.

Usuários internos

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
Conexão interna direta	TCP	Rede do cliente	1024–65535	Rede VDA	443
Conexão interna direta	UDP	Rede do cliente	1024–65535	Rede VDA	443

Usuários externos

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
STUN (somente usuários externos)	UDP	Rede do cliente	1024–65535	Internet (consulte a nota abaixo)	3478, 19302
Conexão de usuário externo	UDP	Rede do cliente	1024–65535	Endereço IP público do data center	1024–65535

Rede do data center

A tabela a seguir descreve a rede do data center para usuários internos e externos.

Usuários internos

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
Conexão interna direta	TCP	Rede do cliente	1024–65535	Rede VDA	443
Conexão interna direta	UDP	Rede do cliente	1024–65535	Rede VDA	443

Usuários externos

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
STUN (somente usuários externos)	UDP	Rede VDA	1024–65535	Internet (ver nota abaixo)	3478, 19302
Conexão de usuário externo	UDP	DMZ / Rede interna	1024–65535	Rede VDA	55000–55250

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
Conexão de usuário externo	UDP	Rede VDA	55000–55250	IP público do cliente	1024–65535

NOTA:

Tanto o VDA quanto o aplicativo Workspace tentam enviar solicitações STUN para os seguintes servidores na mesma ordem:

- stun.cloud.com:3478
- stun.cloudflare.com:3478
- stun.l.google.com:19302

Se você alterar o intervalo de portas padrão para conexões de usuários externos usando a configuração de política **Intervalo de portas HDX Direct**, as regras de firewall correspondentes devem corresponder ao seu intervalo de portas personalizado.

Configuração

O HDX Direct está desativado por padrão. Você pode configurar esse recurso usando a configuração **HDX Direct** na política do Citrix.

- **HDX Direct**: Para ativar ou desativar um recurso.
- **Modo HDX Direct**: Determina se o **HDX Direct** está disponível apenas para clientes internos ou para clientes internos e externos.
- **Intervalo de portas HDX Direct**: Define o intervalo de portas que o VDA usa para conexões de clientes externos.

Se necessário, a lista de servidores STUN usados pelo HDX Direct pode ser modificada editando o seguinte valor de registro:

- Key: HKLM\SOFTWARE\Citrix\HDX-Direct
- Tipo de valor: REG_MULTI_SZ

- Nome do valor: STUNServers
- Dados: stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

> **NOTA:**
>
> O HDX Direct para usuários externos está disponível apenas com EDT (UDP) como protocolo de transporte. Portanto, o Transporte Adaptável deve ser habilitado.

Considerações

A seguir estão as considerações para usar o HDX Direct:

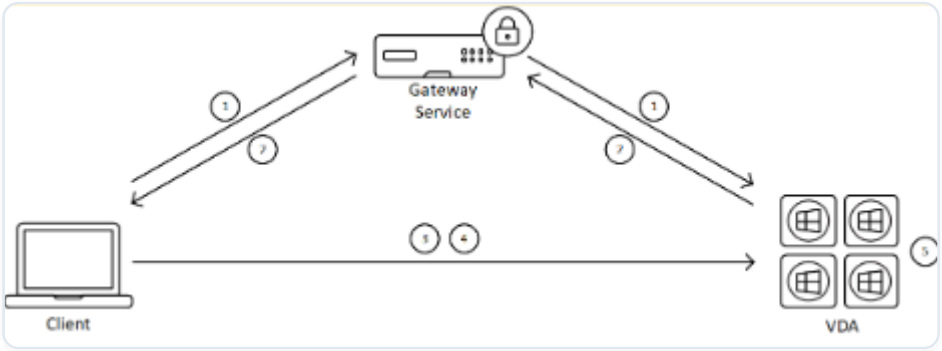
- O HDX Direct para usuários externos está disponível apenas com EDT (UDP) como protocolo de transporte. Portanto, o **Transporte Adaptável** deve ser habilitado.
- Se você estiver usando o **HDX Insight**, observe que o uso do **HDX Direct** impede a coleta de dados do HDX Insight, já que a sessão não seria mais intermediada pelo NetScaler Gateway.

Como funciona

O HDX Direct permite que os clientes estabeleçam uma conexão direta com o host da sessão quando a comunicação direta está disponível. Quando as conexões diretas são feitas usando o HDX Direct, certificados autoassinados são usados para proteger a conexão direta com criptografia em nível de rede (TLS/DTLS).

Usuários internos

O diagrama a seguir descreve a visão geral do processo de conexão do HDX Direct de usuários internos.



1. O cliente estabelece uma sessão HDX através do Gateway Service.
2. Após uma conexão bem-sucedida, o VDA envia ao cliente o FQDN da máquina VDA, uma lista de seus endereços IP e o certificado da máquina VDA via conexão HDX.

3. O cliente sonda os endereços IP para verificar se consegue alcançar o VDA diretamente.
4. Se o cliente conseguir alcançar o VDA diretamente com qualquer um dos endereços IP compartilhados, o cliente estabelece uma conexão direta com o VDA, protegida com (D)TLS usando um certificado que corresponde ao trocado na etapa (2).
5. Uma vez que a conexão direta é estabelecida com sucesso, a sessão é transferida para a nova conexão, e a conexão com o Serviço Gateway é encerrada.

> **Nota:**
>
> Após estabelecer a conexão na etapa 2, acima, a sessão está ativa. As etapas subsequentes não atrasam nem interferem na capacidade do usuário de usar o aplicativo ou desktop virtual. Se alguma das etapas subsequentes falhar, a conexão através do Gateway é mantida sem interromper a sessão do usuário.

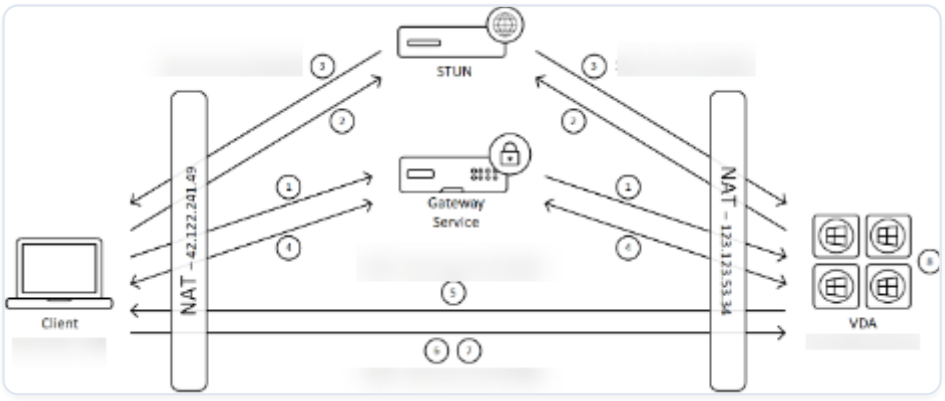
Conexões diretas tradicionais

Ao usar Storefront, Workspace com Conexão Direta de Carga de Trabalho, ou Workspace configurado para conectividade apenas interna, conexões diretas são estabelecidas entre o cliente e o host da sessão sem a necessidade de rotear primeiro por um Gateway.

Nesses casos, o HDX Direct não é acionado, pois as conexões são inerentemente diretas. No entanto, se o HDX Direct estiver habilitado, essas conexões utilizarão os certificados HDX Direct para proteger as sessões.

Usuários externos

O diagrama a seguir descreve a visão geral do processo de conexão HDX Direct para usuários externos:



1. O cliente estabelece uma sessão HDX através do Serviço Gateway.

2. Após uma conexão bem-sucedida, tanto o cliente quanto o VDA enviam uma solicitação STUN para descobrir seus endereços IP públicos e portas.
3. O servidor STUN responde ao cliente e ao VDA com seus respectivos endereços IP públicos e portas.
4. Através da conexão HDX, o cliente e o VDA trocam seus endereços IP públicos e portas UDP, e o VDA envia seu certificado para o cliente.
5. O VDA envia pacotes UDP para o endereço IP público e porta UDP do cliente. O cliente envia pacotes UDP para o endereço IP público e porta UDP do VDA.
6. Ao receber uma mensagem do VDA, o cliente responde com uma solicitação de conexão segura.
7. Durante o handshake DTLS, o cliente verifica se o certificado corresponde ao certificado trocado na etapa (4). Após a validação, o cliente envia seu token de autorização. Uma conexão direta segura é agora estabelecida.
8. Uma vez que a conexão direta é estabelecida com sucesso, a sessão é transferida para a nova conexão, e a conexão com o Serviço Gateway é encerrada.

> **Nota:**
>
> Após estabelecer a conexão na etapa 2, acima, a sessão está ativa. As etapas subsequentes não atrasam nem interferem na capacidade do usuário de usar o aplicativo ou desktop virtual. Se alguma das etapas subsequentes falhar, a conexão através do Gateway é mantida sem interromper a sessão do usuário.

Gerenciamento de certificados

Visão geral

As conexões diretas HDX™ são protegidas com criptografia em nível de rede. Para facilitar isso, cada host de sessão possui um certificado de CA raiz autoassinado exclusivo e um certificado de servidor correspondente, que é assinado pelo certificado de CA raiz autoassinado.

Esta solução oferece as seguintes vantagens:

- **Segurança Simplificada:** As conexões diretas HDX são protegidas sem a sobrecarga administrativa de gerenciar certificados no ambiente.

- **Superfície de Ataque Reduzida:** A superfície de ataque é limitada a um único host porque cada host possui um conjunto exclusivo de chaves e certificados.
- **Segurança Aprimorada para Ambientes Não Persistentes:** Em ambientes com hosts de sessão não persistentes, a segurança é ainda mais aprimorada, pois novas chaves e certificados são gerados a cada reinício.

Host de sessão

O **Citrix ClxMtp Service** e o **Citrix Certificate Manager Service** são os dois serviços responsáveis pelo gerenciamento de certificados em cada host de sessão. O ClxMtp Service lida com a geração e rotação de chaves, enquanto o Certificate Manager Service gera e gerencia os certificados.

Dois certificados são criados: uma CA raiz autoassinada e um certificado de servidor. Ambos são emitidos com um período de validade de dois anos; no entanto, são substituídos quando as chaves são rotacionadas. Além disso, novos certificados são gerados cada vez que máquinas não persistentes são reiniciadas.

Os detalhes de cada certificado são os seguintes:

- **CA Raiz Autoassinada**
  - Emitido para: CA-Citrix-Certificate-Manager
  - Emitido por: CA-Citrix-Certificate-Manager
  - Detalhes do emissor: A organização é Citrix Systems, Inc.
- **Certificado do Servidor**
  - Emitido para: \<host FQDN\> (Por exemplo, FTLW11-001.ctxlab.net)
  - Emitido por: CA-Citrix-Certificate-Manager
  - Detalhes do emissor: A organização é Citrix Systems, Inc.

> **NOTA:**

> O Serviço Citrix Certificate Manager gera certificados RSA que utilizam chaves de 2048 bits.

> Se houver um certificado de máquina existente criado pelo Serviço Citrix Certificate Manager e o nome do assunto não corresponder ao FQDN da máquina, um novo certificado será gerado.

Rotação de chaves

O **Serviço Citrix ClxMtp** gira automaticamente as chaves a cada seis meses. No entanto, você pode acionar uma rotação de chave manualmente aumentando o contador de rotação no registro do host da sessão.

Para girar as chaves, atualize o seguinte valor:

- Chave: SOFTWARE\Citrix\ClxMtpConnectorSvcRotateKeyPairs
- Tipo de valor: DWORD
- Nome do valor: ClxMtpRotateRequestCounter
- Dados: integer (Decimal)

NOTA:

Para a primeira rotação de chave:

1. Crie a chave ClxMtpConnectorSvcRotateKeyPairs.
2. Crie e defina o valor ClxMtpRotateRequestCounter como 1.

Para rotações de chave subsequentes, aumente o valor ClxMtpRotateRequestCounter em 1.

Assim que o valor for atualizado, o **Citrix ClxMtp Service** rotacionará automaticamente as chaves sem exigir uma reinicialização. O **Citrix Certificate Manager Service** gerará novos certificados automaticamente assim que detectar novas chaves.

Dispositivo cliente

O certificado raiz da CA é enviado ao cliente pelo Citrix® StoreFront Cloud ou Citrix® StoreFront através do caminho de conexão seguro e confiável já estabelecido. Isso elimina a necessidade de distribuir certificados de CA para os armazenamentos de certificados dos dispositivos cliente e garante que o cliente confie nos certificados usados para proteger a conexão HDX Direct.

Usando certificados personalizados

O HDX Direct oferece suporte ao uso de certificados emitidos e gerenciados por sua própria PKI. As etapas a seguir descrevem como instalar seu certificado, configurar as permissões necessárias, vinculá-lo ao serviço de gerenciador de sessão e habilitar os ouvintes TLS necessários.

1. Prossiga para a etapa 2 se o HDX Direct estiver desabilitado na máquina. Se o HDX Direct estiver habilitado, siga as etapas abaixo:
    a. Abra o editor do Registro (regedit.exe) e navegar até **HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**.
    b. Defina o valor **SSLEnabled** como **0**.
    c. navegar até **HKLM\Software\Citrix\HDX-Direct**.
    d. Defina o valor **HdxDirectCaInTls** como **0**.
2. Instale o certificado apropriado emitido pela sua PKI no armazenamento de certificados da máquina.
3. Conceda ao serviço de gerenciador de sessão acesso de leitura às chaves privadas do certificado.
    a. Inicie o console de gerenciamento da Microsoft (**MMC**): Iniciar > Executar > mmc.exe.
    b. navegar até **Arquivo > Adicionar/Remover Snap-in**.
    c. Selecione **Certificados** e clique em **Adicionar**.
    d. Escolha **Conta de computador** e clique em **Avançar**.
    e. Selecione **Computador local** e clique em **Concluir**.
    f. navegar até **Certificados (Computador Local) > Pessoal > Certificados**.
    g. Clique com o botão direito do mouse no certificado apropriado e selecione **Todas as Tarefas > Gerenciar Chaves Privadas**.
    h. Adicione um dos seguintes serviços e conceda a ele acesso de Leitura:
        - Para **VDA de Sessão Única**: `NT SERVICE\PorticaService`
        - Para **VDA de Múltiplas Sessões**: `NT SERVICE\TermService`
    i. Clique em **Aplicar** e depois em **OK**.
4. Vincule o certificado ao serviço de gerenciador de sessão.

a. Recupere o thumbprint do certificado (clique duas vezes no certificado > **Detalhes** > **Thumbprint**).

b. Abra o editor do Registro (regedit.exe) e navegar até **HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**.

c. Edite o valor de **SSLThumbprint** e cole o thumbprint do certificado.

5. Habilite os ouvintes TLS da Citrix.

   a. No mesmo local do registro, defina o valor de **SSLEnabled** como **1**.

6. Habilite o HDX Direct (na política Citrix).

A mídia de instalação do Citrix Virtual Apps and Desktops inclui um script PowerShell (Enable-VdaSSL.ps1) que automatiza várias dessas tarefas:

- Definir permissões para as chaves do certificado
- Vincular o certificado ao serviço do gerenciador de sessão
- Habilitar os ouvintes TLS da Citrix

Este script está localizado no diretório Support > Tools > SslSupport. Para mais detalhes, consulte Configurar TLS em um VDA usando o script PowerShell.

> **NOTA:**
>
> Os dispositivos que se conectam aos hosts de sessão precisam ter os certificados de CA raiz e CA intermediária corretos instalados se você estiver usando seus próprios certificados.

Compatibilidade NAT

Para estabelecer uma conexão direta entre um dispositivo de usuário externo e o host da sessão, o HDX™ Direct utiliza o hole punching para travessia NAT e o STUN para facilitar a troca do endereço IP público e dos mapeamentos de porta para o dispositivo cliente e o host da sessão. Isso é semelhante ao funcionamento de soluções de VoIP, comunicações unificadas e P2P.

Desde que os firewalls e outros componentes de rede estejam configurados para permitir o tráfego UDP para as solicitações STUN e as sessões HDX, espera-se que o HDX Direct para usuários externos funcione. No entanto, existem certos cenários em que os tipos de NAT das redes do usuário e do host da sessão levam a uma combinação incompatível, fazendo com que o HDX Direct falhe.

Validações

Você pode validar o tipo e o filtro NAT no cliente e no host da sessão usando o utilitário cliente STUN do STUNTMAN:

1. Baixe o pacote apropriado para a plataforma de destino em stunprotocol.org e extraia o conteúdo.
2. Abra um prompt de terminal e navegar até o diretório onde o conteúdo foi extraído.
3. Execute o seguinte comando: `.\stunclient.exe stunserver.stunprotocol.org --mode behavior`
4. Anote a saída.

   Se os testes de binding e comportamento forem bem-sucedidos, tanto o **teste de binding** quanto o **teste de comportamento** relatam o sucesso e um comportamento NAT é especificado:

   Se os testes falharem, tanto o **teste de binding** quanto o **teste de comportamento** relatam a falha.

5. Execute o seguinte comando: `.\stunclient.exe stunserver2024.stunprotocol.org --mode filtering`
6. Anote a saída.

Consulte a tabela a seguir para determinar se o HDX Direct para usuários externos deve funcionar com base nos resultados do teste do cliente e do host da sessão:

COMPORTAMENTO NAT DO CLIENTE	FILTRAGEM NAT DO CLIENTE	COMPORTAMENTO NAT DO HOST DA SESSÃO	FILTRAGEM NAT DO HOST DA SESSÃO	ESPERADO QUE FUNCIONE?
Mapeamento Independente de Endpoint	Qualquer	Mapeamento Independente de Endpoint	Qualquer	Sim
Mapeamento Independente de Endpoint	Filtragem Independente de Endpoint	Mapeamento Dependente de Endereço	Qualquer	Sim
Mapeamento Independente de Ponto de Extremidade	Filtragem Dependente de Endereço	Mapeamento Dependente de Endereço	Qualquer	Não
Mapeamento Independente de Ponto de Extremidade	Filtragem Dependente de Endereço e Porta	Mapeamento Dependente de Endereço	Qualquer	Não
Mapeamento Independente de Ponto de Extremidade	Filtragem Independente de Ponto de Extremidade	Mapeamento Dependente de Endereço e Porta	Filtragem Independente de Ponto de Extremidade	Sim
Mapeamento Independente de Endpoint	Filtragem Dependente de Endereço	Mapeamento Dependente de Endereço	Qualquer	Não
Mapeamento Independente de Endpoint	Filtragem Dependente de Endereço e Porta	Mapeamento Dependente de Endereço	Qualquer	Não
Mapeamento Dependente de Endereço	Qualquer	Mapeamento Independente de Endpoint	Filtragem Independente de Endpoint	Sim

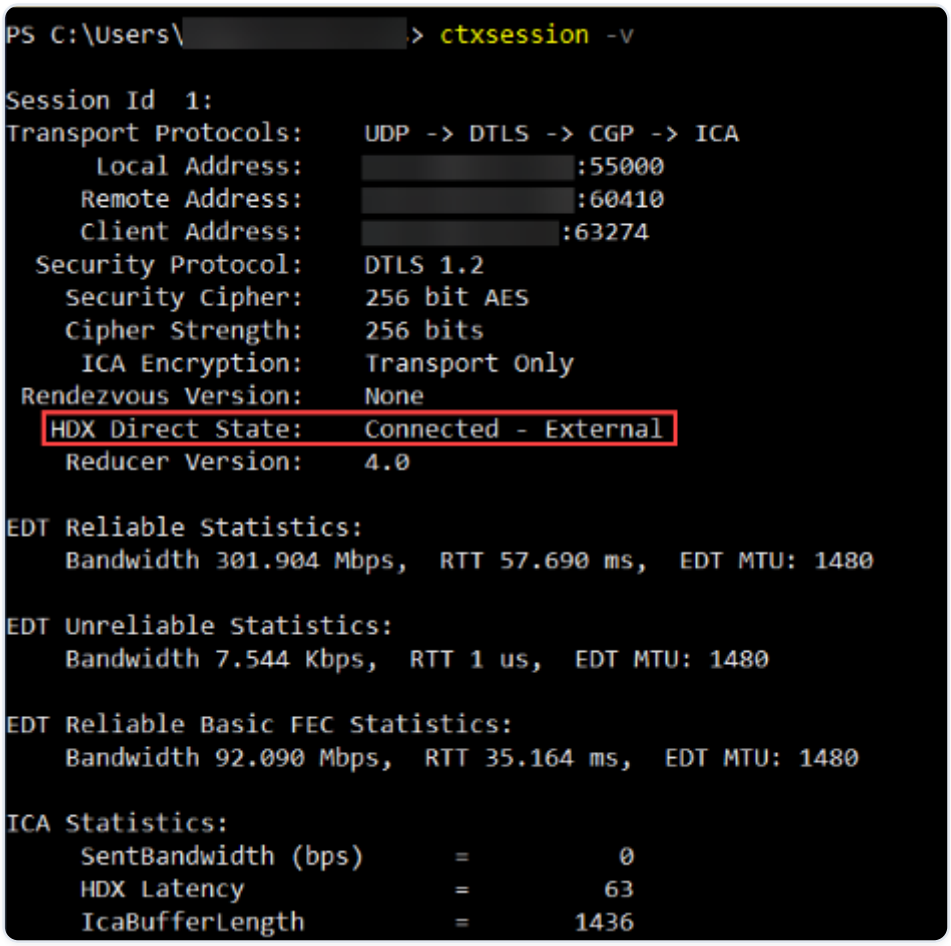
COMPORTAMENTO NAT DO CLIENTE	FILTRAGEM NAT DO CLIENTE	COMPORTAMENTO NAT DO HOST DA SESSÃO	FILTRAGEM NAT DO HOST DA SESSÃO	ESPERADO QUE FUNCIONE?
Mapeamento Dependente de Endereço	Qualquer	Mapeamento Independente de Ponto de Extremidade	Filtragem Dependente de Endereço	Não
Mapeamento Dependente de Endereço	Qualquer	Mapeamento Independente de Ponto de Extremidade	Filtragem Dependente de Endereço e Porta	Não
Mapeamento Dependente de Endereço	Qualquer	Mapeamento Dependente de Endereço	Qualquer	Não
Mapeamento Dependente de Endereço	Qualquer	Mapeamento Dependente de Endereço e Porta	Qualquer	Não
Mapeamento Dependente de Endereço e Porta	Qualquer	Mapeamento Independente de Endpoint	Filtragem Independente de Endpoint	Sim
Mapeamento Dependente de Endereço e Porta	Qualquer	Mapeamento Independente de Endpoint	Filtragem Dependente de Endereço	Não
Mapeamento Dependente de Endereço e Porta	Qualquer	Mapeamento Independente de Endpoint	Filtragem Dependente de Endereço e Porta	Não
Mapeamento Dependente de Endereço e Porta	Qualquer	Mapeamento Dependente de Endereço	Qualquer	Não

COMPORTAMENTO NAT DO CLIENTE	FILTRAGEM NAT DO CLIENTE	COMPORTAMENTO NAT DO HOST DA SESSÃO	FILTRAGEM NAT DO HOST DA SESSÃO	ESPERADO QUE FUNCIONE?
Mapeamento Dependente de Endereço e Porta	Qualquer	Mapeamento Dependente de Endereço e Porta	Qualquer	Não
Falha	Qualquer	Qualquer	Qualquer	Não
Qualquer	Qualquer	Falha	Qualquer	Não
Falha	Qualquer	Falha	Qualquer	Não

Solução de problemas

Para confirmar que o **HDX Direct** estabeleceu com sucesso uma conexão direta, você pode usar o utilitário `CtxSession.exe` na máquina VDA.

Para usar o utilitário `CtxSession.exe`, inicie um Prompt de Comando ou PowerShell dentro da sessão e execute `ctxsession.exe -v`. Se a conexão **HDX Direct** for estabelecida com sucesso, o **HDX Direct Status** será `Connected`.



Você também pode consultar os logs de eventos do host da sessão para obter informações sobre se a conexão HDX™ Direct foi estabelecida com sucesso ou falhou. Consulte a seção **Logs de Eventos** para obter detalhes.

> Nota:
>
> Dependendo do ambiente e do número de endereços IP disponíveis para os hosts da sessão, pode levar até 5 minutos para que a conexão HDX Direct seja estabelecida.

Quando o HDX Direct falha ao estabelecer uma conexão direta

Se o HDX Direct estiver falhando ao estabelecer uma conexão direta, revise as seguintes etapas:

1. Certifique-se de que a versão do VDA e a versão do aplicativo Workspace em uso suportam o recurso de acordo com os requisitos do sistema.
2. Confirme que você tem uma política aplicada ao VDA que habilita o HDX Direct e que não há outras políticas com prioridade mais alta desabilitando o recurso.
3. Confirme que você tem uma política aplicada ao VDA que define o modo HDX Direct desejado e que não há outras políticas com prioridade mais alta sobrescrevendo a configuração.

4. Certifique-se de que o Serviço Citrix ClxMtp esteja em execução no host da sessão.
5. Certifique-se de que o Serviço Citrix Certificate Manager esteja em execução no host da sessão. Se não estiver em execução, tente iniciá-lo manualmente. O serviço para automaticamente se o HDX Direct for desabilitado.
6. Verifique se o host da sessão possui seu certificado de CA Raiz autoassinado:
    a. Emitido para: `CA-<hostname>` (Por exemplo, CA-FTLW11-001)
    b. Emitido por: `CA-<hostname>` (Por exemplo, CA-FTLW11-001)
    c. Detalhes do emissor: A organização é Citrix Systems, Inc.
7. Verifique se o host da sessão possui seu certificado de servidor autoassinado:
    a. Emitido para: `<host FQDN>` (Por exemplo, FTLW11-001.ctxlab.net)
    b. Emitido por: `CA-<hostname>` (Por exemplo, CA-FTLW11-001)
    c. Detalhes do emissor: A organização é Citrix Systems, Inc.
8. Se os certificados estiverem ausentes, entre em contato com o Suporte Técnico da Citrix.
9. Se os certificados estiverem presentes:
    a. Pare o serviço Citrix Certificate Manager no host da sessão.
    b. Exclua tanto o certificado de CA Raiz autoassinado quanto o certificado de servidor autoassinado.
    c. Inicie o serviço Citrix Certificate Manager no host da sessão. O serviço cria novos certificados assim que é iniciado.
10. Para usuários internos:
    a. Certifique-se de que o firewall do host da sessão não esteja bloqueando o tráfego de entrada nas portas UDP 443 ou TCP 443, para HDX over EDT e HDX over TCP, respectivamente.
    b. Certifique-se de que o firewall da sua rede não esteja bloqueando o tráfego nas portas UDP 443 e TCP 443 entre a rede dos seus clientes e a rede dos hosts da sessão.
11. Para usuários externos:
    a. Verifique o tipo de NAT para o cliente e o host da sessão e certifique-se de que a combinação deve funcionar. Consulte a seção Compatibilidade de NAT para obter detalhes.

b. Se o teste de NAT falhar no cliente ou no host da sessão:

   i. Se houver um firewall em execução no sistema, certifique-se de que ele não esteja bloqueando o tráfego de saída na porta UDP 3478.

   ii. Certifique-se de que seus firewalls de rede não estejam bloqueando o tráfego de saída na porta UDP 3478.

   iii. Certifique-se de que os firewalls não estejam bloqueando a resposta do servidor STUN.

c. Certifique-se de que seus firewalls de rede tenham as regras apropriadas configuradas para permitir todo o tráfego necessário. Consulte a seção Requisitos de Rede para obter detalhes.

d. Se você alterar o intervalo de portas padrão usando a configuração de política de intervalo de portas HDX Direct, certifique-se de que suas regras de firewall estejam definidas para o intervalo de portas personalizado.

Logs de eventos

Os seguintes eventos são registrados no log de eventos da máquina VDA:

LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
Logs de Aplicativos e Serviços > Citrix-HostCore-HDX Direct/ Operational	1	HDX Direct	Informações	Conexão HDX Direct para o usuário interno `<username>` estabelecida.
Logs de Aplicativos e Serviços > Citrix-HostCore-HDX Direct/ Operational	2	HDX Direct	Informações	Conexão HDX Direct para o usuário externo `<username>` estabelecida.
Logs de Aplicativos e Serviços > Citrix-HostCore-HDX	3	HDX Direct	Informações	Conexão HDX Direct para o usuário

LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
Direct/ Operational				`<username>` falhou.
Logs de Aplicativos e Serviços > Citrix-HostCore-HDX Direct/ Operational	4	HDX Direct	Informação	O servidor STUN `<URL:PORT>` forneceu o seguinte mapeamento de IP e PORTA do host de sessão para o usuário `<username>`: `<IP>:<PORT>` .
Logs de Aplicativos e Serviços > Citrix-HostCore-HDX Direct/ Operational	5	HDX Direct	Informação	Nenhuma resposta recebida pelo host de sessão de nenhum dos servidores STUN configurados para o usuário `<username>`.
Logs de Aplicativos e Serviços > Citrix-HostCore-HDX Direct/ Operational	6	HDX Direct	Informação	O cliente forneceu `<IP>:<PORT>` como mapeamento externo para o usuário `<username>`.
Registros de Aplicativos e Serviços > Citrix-	7	HDX Direct	Informações	Nenhum mapeamento externo foi fornecido pelo

LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
HostCore-HDX Direct/ Operational				cliente para o usuário `<username>`.

Problemas conhecidos

O HDX Direct pode parar de funcionar após realizar um upgrade in-place do VDA em uma máquina que já tem o **HDX Direct** ativado. Para resolver o problema, conclua as seguintes etapas:

1. Pare o serviço Citrix Certificate Manager no host da sessão.
2. Exclua o certificado autoassinado da CA Raiz e o certificado de servidor autoassinado.
3. Abra o registro.
4. Exclua a chave `HKLM\Software\Citrix\HDX-Direct`.
5. Vá para `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`.
6. Defina o valor **SSLEnabled** como `0`.
7. Exclua o conteúdo do valor **SSLThumbprint**.
8. Inicie o **Serviço Citrix Certificate Manager**.

HDX Seguro™

O HDX Seguro é uma solução de Criptografia em Nível de Aplicativo (ALE) que impede que quaisquer elementos de rede no caminho do tráfego inspecionem o tráfego HDX. Isso é feito fornecendo Criptografia de Ponta a Ponta (E2EE) verdadeira no nível do aplicativo entre o aplicativo Citrix Workspace™ (cliente) e o VDA (host de sessão) usando criptografia AES-256-GCM.

Requisitos do sistema

A lista a seguir descreve os requisitos do sistema para usar o HDX Seguro.

- Plano de controle
  - Citrix DaaS™
  - Citrix Virtual Apps and Desktops™ 2503 ou posterior
- Host de sessão

    - Sistema operacional
        - Windows 10 22H2
        - Windows 11 22H2 ou posterior
        - Windows Server 2019 ou posterior
    - Virtual Delivery Agent (VDA)
        - Windows: versão 2503 ou posterior
        - Linux: versão 2407 ou posterior
- Aplicativo Workspace
    - Windows: versão 2503 ou posterior
    - Linux: versão 2408 ou posterior
    - Mac: versão 2409 ou posterior
    - Chrome OS: versão 2409 ou posterior
    - HTML5: versão 2408 ou posterior
    - Android: versão 2503 ou posterior
    - iOS: versão 2503 ou posterior
- Camada de acesso
    - Citrix® StoreFront Cloud
    - Citrix StoreFront 2402 ou posterior

> **NOTA:**

> Para obter detalhes sobre a configuração do Secure HDX com Linux VDA, consulte a documentação do Linux VDA.

Configuração

O Secure HDX está desativado por padrão. Você pode configurar esse recurso usando a configuração Secure HDX na política do Citrix:

Secure HDX: Define se o recurso deve ser ativado ou desativado.

> **IMPORTANTE:**
>
> Se você tiver o Secure ICA® ativado nos grupos de entrega nos quais deseja ativar o Secure HDX, você deve primeiro desativar o Secure ICA (Editar grupo de entrega > Configurações do usuário).

HDX Insight e Smart Control

A seguir estão os requisitos para usar o HDX Insight e o SmartControl com o NetScaler Gateway quando o Secure HDX estiver ativado:

- NetScaler 14.1 Build 47.46 ou mais recente (14.1 Build 72.57 ou mais recente necessário para suporte a EDT).
- **Telemetria de rede** deve ser ativada na política do Citrix. Consulte Telemetria de rede para obter detalhes.
- **Confiabilidade da Sessão** deve ser ativada. Essa configuração é ativada por padrão, portanto, certifique-se de que não haja políticas desativando-a.

> **Nota:**
>
> O HDX Insight e o SmartControl com Secure HDX estão disponíveis apenas nos seguintes cenários:
>
> - Ao usar o NetScaler 14.1 Build 47.46 ou mais recente (14.1 Build 72.57 ou mais recente necessário para EDT)
> - Conexões usando IPv4

Considerações

A seguir estão as considerações para usar o Secure HDX:

- Se um usuário tentar se conectar a um host de sessão com o Secure HDX ativado usando um cliente que não oferece suporte ao recurso, a conexão será negada.
- Apenas Service Continuity para cargas de trabalho sem conector é suportado com o Secure HDX. Se você estiver usando a versão padrão do Service Continuity, não conseguirá se

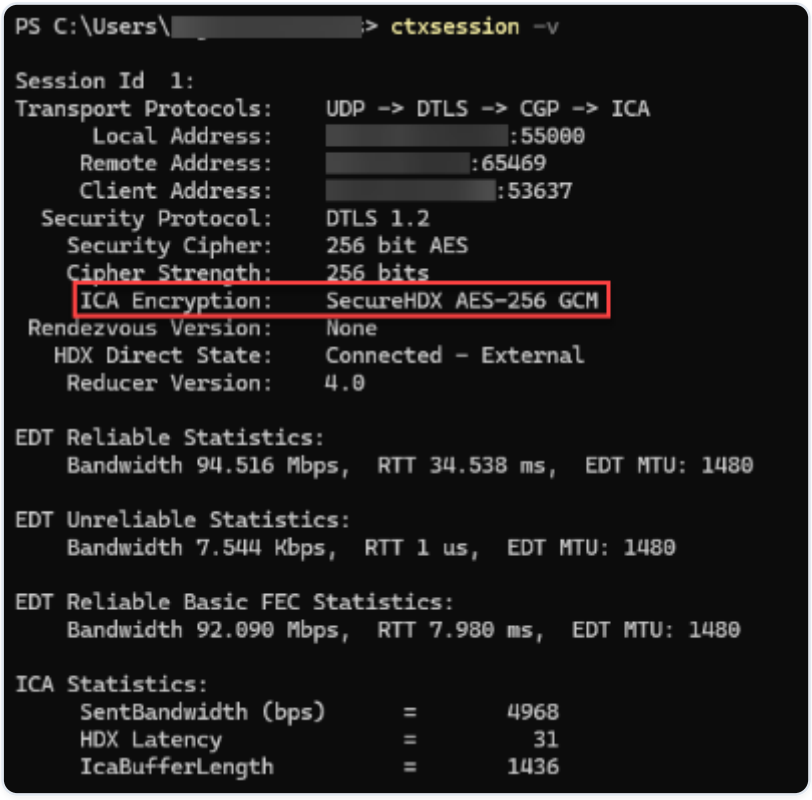
conectar a nenhum host de sessão que tenha o Secure HDX ativado se houver uma interrupção do serviço de nuvem.

- O ICA Multi-Stream não é suportado quando o Secure HDX está ativado.
- Se você usar soluções de terceiros que dependem da inspeção do tráfego HDX, elas não funcionarão mais se você ativar o Secure HDX, pois o tráfego HDX é criptografado.

Solução de problemas

Para confirmar que o Secure HDX está ativo, você pode usar o utilitário `ctxsession.exe` na máquina VDA.

Para usar o utilitário `CtxSession.exe`, abra um Prompt de Comando ou PowerShell dentro da sessão e execute `ctxsession.exe -v`. Se o Secure HDX estiver em uso, a Criptografia ICA exibirá `SecureHDX AES-256 GCM`.



Quando o Secure HDX não é ativado na sessão

- Certifique-se de que a versão do VDA em uso suporte o recurso de acordo com os requisitos do sistema.
- Confirme se você tem uma política aplicada ao VDA que habilita o Secure HDX e que não há outras políticas com prioridade mais alta desativando o recurso.

- Se o host da sessão já estava em execução quando você configurou o Secure HDX, reinicie a máquina para garantir que as alterações entrem em vigor.

Telemetria de rede

As métricas de rede são críticas para a solução de problemas de sessão Citrix porque o desempenho e a estabilidade de uma sessão Citrix dependem muito das condições da rede subjacente. Ao contrário de um aplicativo local, uma sessão Citrix envolve o streaming de uma experiência interativa de desktop ou aplicativo por uma rede, o que significa que qualquer instabilidade ou gargalo na rede impactará diretamente a percepção de desempenho do usuário.

Para obter detalhes sobre as métricas de rede disponíveis no Citrix Monitor e Director, consulte Diagnosticar problemas de desempenho da sessão.

Requisitos do sistema

A seguir estão os requisitos do sistema para usar a Telemetria de Rede:

- Plano de controle
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2503 ou posterior
- Virtual Delivery Agent (VDA)
  - Windows: versão 2503 ou posterior
  - Linux: versão 2507 ou posterior
  - Mac: versão 2507 ou posterior
- Aplicativo Workspace
  - Windows: versão 2503 ou posterior
  - Linux: versão 2508 ou posterior
  - Mac: versão 2505 ou posterior
- Camada de acesso
  - Citrix® StoreFront Cloud
  - Citrix StoreFront 2402 ou posterior
  - Citrix Gateway Service

- Citrix NetScaler Gateway 14.1 Build 47.46 ou posterior (14.1 Build 72.57 ou posterior necessário para suporte a EDT)

Requisitos de rede

Se você estiver usando o Citrix Gateway Service, não há requisitos de rede adicionais. No entanto, se você estiver usando o NetScaler Gateway, há requisitos adicionais para usar a Telemetria de Rede, que são descritos abaixo.

Hosts de sessão

Se seus hosts de sessão tiverem um firewall, como o Firewall do Windows Defender, você deverá permitir o seguinte tráfego de entrada para conexões do NetScaler Gateway.

DESCRIÇÃO	ORIGEM	PROTOCOLO	PORTA
Conexão do NetScaler Gateway	NetScaler SNIP	UDP	443
Conexão do NetScaler Gateway	NetScaler SNIP	TCP	443

NOTA:

O instalador do VDA adiciona as regras de entrada apropriadas ao Firewall do Windows Defender. Se você usar um firewall diferente, deverá adicionar as regras acima.

Rede interna

A seguir estão os requisitos de firewall para sua rede interna:

DESCRIÇÃO	PROTOCOLO	ORIGEM	PORTA DE ORIGEM	DESTINO	PORTA DE DESTINO
Conexão do NetScaler Gateway	UDP	SNIP do NetScaler	1024-65535	Rede VDA	443
Conexão do NetScaler Gateway	TCP	SNIP do NetScaler	1024-65535	Rede VDA	443

Configuração

A telemetria de rede está desabilitada por padrão. Você pode configurar este recurso através da política Citrix no Studio usando a seguinte configuração.

- **Telemetria de rede:** define se o recurso deve ser habilitado ou desabilitado.

Considerações

As seguintes são considerações para usar a Telemetria de Rede:

- Para garantir que os dados de monitoramento permaneçam seguros em trânsito, as conexões do NetScaler Gateway para os hosts de sessão são protegidas com TLS/DTLS quando a Telemetria de Rede está habilitada. Como resultado, as conexões são estabelecidas nas portas UDP 443 (HDX sobre EDT) e TCP 443 (HDX sobre TCP) por padrão. Consulte Recursos HDX gerenciados através do registro se desejar alterar o número da porta.
- Certificados autogerenciados são usados para facilitar a criptografia em nível de rede para conexões de sessão. Consulte Gerenciamento de certificados HDX Direct para obter detalhes sobre o gerenciamento de certificados. Observe que habilitar a Telemetria de Rede não habilita o HDX Direct.
- A Telemetria de Rede para EDT é suportada com a versão do NetScaler **14.1 Build 72.57** e mais recente. Se você estiver usando uma versão mais antiga do NetScaler, as sessões serão forçadas a usar TCP se a Telemetria de Rede estiver habilitada.

Lista de permissões de canal virtual

A lista de permissões de canal virtual é um recurso que permite controlar quais canais virtuais não-Citrix são permitidos em seu ambiente. Por padrão, o recurso de lista de permissões de canal virtual está habilitado. Como resultado, apenas os canais virtuais Citrix têm permissão para abrir em sessões do Citrix Virtual Apps and Desktops™. Se houver necessidade de usar canais virtuais personalizados, sejam eles desenvolvidos internamente ou de terceiros, eles precisam ser adicionados explicitamente à lista de permissões.

Configuração

A lista de permissões de canal virtual é habilitada por padrão. Você pode configurar esse recurso usando as seguintes configurações na política Citrix:

- **Lista de permissões de canal virtual**: para habilitar ou desabilitar o recurso e adicionar canais virtuais à lista.

- **Limitação de log da lista de permissões de canal virtual**: define o período de limitação para o registro de eventos da lista de permissões de canal virtual.
- **Registro em log da lista de permissões de canal virtual**: define o nível de registro em log para a lista de permissões de canal virtual.

Adicionando canais virtuais à lista de permissões

Para adicionar um canal virtual à lista de permissões, você precisa das seguintes informações:

1. O nome do canal virtual conforme definido no código, que pode ter até sete caracteres. Por exemplo, `CTXCVC1`.
2. Os caminhos para os processos que abrem o canal virtual na máquina VDA. Por exemplo, `C:\Program Files\Application\run.exe`.

Depois de ter as informações necessárias, você deve adicionar o canal virtual à lista de permissões usando a configuração de política da lista de permissões de canal virtual. Para adicionar um canal virtual à lista, insira o nome do canal virtual seguido por uma vírgula e, em seguida, o caminho para o processo que acessa o canal virtual. Se houver vários processos, você pode adicioná-los separando cada processo com vírgulas.

Para processos únicos

Usando os exemplos anteriores, adicione a seguinte entrada à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Para vários processos

Se houver vários processos, adicione a seguinte entrada à lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

Usando curingas

O uso de curingas (*) é suportado. Você pode usar curingas quando os nomes de diretórios ou executáveis mudam com base na versão do aplicativo, ou se o componente de terceiros estiver instalado nos perfis dos usuários.

Você pode usar curingas nos seguintes cenários:

- Para substituir o nome completo do diretório. Por exemplo: `C:\Program Files\Application*\run1.exe`

- Para substituir parte do nome do diretório. Por exemplo: `C:\Program Files\Application\v*\run1.exe`
- Para substituir o nome do executável. Por exemplo: `C:\Program Files\Application\v1.2*.exe`
- Para substituir parte do nome do executável. Por exemplo: `C:\Program Files\Application\v1.2\run*.exe`

As seguintes restrições se aplicam:

- O curinga só pode ser usado para substituir um único diretório. Por exemplo, se o executável estiver localizado em `C:\Program Files\Application\v1.2\run1.exe`
  - Permitido: `C:\Program Files\Application*\run1.exe`
  - Não permitido: `C:\Program Files*\run1.exe`
- As entradas devem conter a extensão do nome do arquivo.
  - Permitido: `C:\Program Files\Application\v1.2*.exe`
  - Não permitido: `C:\Program Files\Application\v1.2*`
- Todos os caminhos devem ser locais.

Nota:

- Caminhos de rede não são permitidos.
- O suporte a curingas está disponível a partir do Citrix Virtual Apps and Desktops 2206.
- O suporte a curingas está disponível no Citrix Virtual Apps and Desktops 2203 LTSR a partir do CU2.

Usando variáveis de ambiente do sistema

Você pode usar variáveis de ambiente do sistema para simplificar a definição dos processos confiáveis em sua lista de permissões. Você pode usar qualquer uma das variáveis prontas para uso, como `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` e `%systemroot%`.

Você também pode usar variáveis de ambiente personalizadas, desde que sejam definidas no nível do sistema.

Os exemplos a seguir descrevem variáveis de ambiente prontas para uso:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

O exemplo a seguir descreve uma variável de ambiente de sistema personalizada:

- Nome da variável personalizada: `app`
- Valor da variável personalizada: `%programfiles%\Application\`
- Entrada da lista de permissões: `CTXCVC1,%app%\run.exe`

> **Nota:**
>
> Variáveis de ambiente de usuário não são suportadas.

> O suporte a variáveis de ambiente está disponível a partir do Citrix Virtual Apps and Desktops versão 2209.

Obter nomes e processos de canais virtuais

A maneira mais fácil de obter o nome do canal virtual e o processo que o abre na máquina VDA é obter as informações do desenvolvedor ou de um fornecedor terceirizado que forneceu o canal virtual.

Alternativamente, você pode obter informações aplicando os logs do recurso e seguindo estas etapas:

1. Depois que os componentes cliente e servidor do canal virtual personalizado estiverem instalados, inicie um aplicativo virtual ou desktop virtual.
2. No log de eventos do sistema da máquina VDA, procure o nome do canal virtual personalizado e o processo que tentou abri-lo. Para obter mais informações sobre os eventos disponíveis, consulte Logs de eventos.
3. Faça logoff da sessão.
4. Adicione uma entrada nas configurações da política de lista de permissões de canais virtuais para o canal virtual e o processo identificados.

5. Reinicie a máquina.
6. Depois que o VDA for registrado, execute o aplicativo virtual ou desktop virtual para validar se os canais virtuais personalizados são abertos com sucesso.

Considerações para canais virtuais Citrix

Todos os canais virtuais Citrix integrados são confiáveis e podem ser abertos sem configuração adicional. No entanto, os dois recursos a seguir exigem entradas explícitas na lista de permissões devido a dependências externas:

- Redirecionamento Multimídia
- Pacote de Otimização HDX RealTime para Skype for Business

Redirecionamento Multimídia

Se você usar um reprodutor de mídia diferente do Windows Media Player como seu reprodutor de mídia do sistema, precisará adicioná-lo à lista de permissões como um processo confiável. As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXMM`
- Processo: Caminho para o reprodutor de mídia usado em sua máquina VDA. Por exemplo, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Entrada da lista de permissões: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

Pacote de Otimização HDX RealTime para Skype for Business

As seguintes informações são necessárias para a entrada da lista de permissões:

- Nome do canal virtual: `CTXRMEP`
- Processo: Caminho para o executável do Skype for Business em sua máquina VDA, que pode variar dependendo da versão do Skype for Business ou se você usou um caminho de instalação personalizado. Por exemplo, `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- Entrada da lista de permissões: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Considerações para canais virtuais de terceiros

A partir da versão 2603 do VDA, canais virtuais de terceiros selecionados são confiáveis e podem ser abertos sem configuração adicional. Todos os outros canais virtuais de terceiros exigem entradas explícitas na lista de permissões. Os canais virtuais de terceiros confiáveis são:

- Microsoft Teams
- Reuniões do Zoom para VDI

> **IMPORTANTE:**
>
> Os canais virtuais de terceiros confiáveis são automaticamente confiáveis apenas quando os aplicativos associados são instalados em seus caminhos de instalação padrão. Se os aplicativos forem instalados em um caminho diferente, você deve adicionar explicitamente os canais virtuais à lista de permissões.

Microsoft Teams

A seguir estão os canais virtuais do Microsoft Teams e o caminho de instalação padrão dos processos:

- Nomes dos canais virtuais: `MSTEAMS`, `MSTEAM1` e `MSTEAM2`
- Processo: `ms-teams.exe`
- Caminho de instalação padrão: `C:\Program Files\WindowsApps\MSTeams.<app version>_x64_8wekyb3d8bbwe\`

Informações adicionais sobre os canais virtuais do Microsoft Teams estão disponíveis na documentação da Microsoft.

Reuniões do Zoom para VDI

A seguir estão os canais virtuais do Zoom Meetings para VDI e o caminho de instalação padrão dos processos:

- Nomes dos canais virtuais: `ZOOMHDX`, `ZOOMHDC`, `ZOOMPHX`, `ZOOMCVX`, `ZOOMCCX`, `ZOOMAUS`
- Processos: `Zoom.exe` e `ZoomVDITool.exe`
- Caminho de instalação padrão:

- 32 bits: `C:\Program Files (x86)\ZoomVDI\bin\`
- 64 bits: `C:\Program Files\ZoomVDI\bin\`

Informações adicionais sobre os canais virtuais do Zoom Meetings for VDI estão disponíveis na documentação do Zoom.

Solução de problemas

Se o seu canal virtual personalizado não abrir, revise as seguintes etapas:

1. Certifique-se de que está usando a versão correta do VDA.
2. Confirme se você tem uma política aplicada ao VDA com o canal virtual personalizado na lista de permissões de canais virtuais e que não há outras políticas com prioridade mais alta sobrescrevendo esta configuração.
3. Verifique o log de eventos no VDA e confirme se o nome do canal virtual relatado corresponde ao definido na lista de permissões.
    a. Se você tiver vários processos, certifique-se de que eles estejam definidos corretamente, conforme descrito em Adicionar canais virtuais à lista de permissões.
    b. Se você estiver usando curingas no caminho do processo definido, certifique-se de que está seguindo as diretrizes para Usar curingas.
    c. Se você estiver usando variáveis de ambiente no caminho do processo definido, certifique-se de que está seguindo as diretrizes em Usar variáveis de ambiente do sistema.

Logs de eventos

Os seguintes eventos são registrados no log de eventos da máquina VDA.

VDA de sessão única

Os seguintes eventos são registrados no log de eventos da máquina VDA de sessão única:

NOME DO LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
Sistema	2001	`Picadd`	Informação	O canal virtual personalizado `<vcName>` foi aberto pelo processo `<processName>`

NOME DO LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
Sistema	2002	`Picadd`	Aviso	O canal virtual personalizado `<vcName>` não pode ser aberto pelo processo `<processName>`
Sistema	2003	`Picadd`	Informação	`<username>` abriu o canal virtual personalizado `<vcName>`
Sistema	2004	`Picadd`	Aviso	`<username>` tentou abrir o canal virtual personalizado `<vcName>`
Sistema	2005	`Picadd`	Erro	O caminho fornecido na política `<pathInPolicy>` não pode ser resolvido para o caminho do processo
Sistema	2007	`Picadd`	Informação	O caminho do processo carregado é `<processPath>`
Sistema	2008	`Picadd`	Erro	Variável de ambiente `<varName>` no caminho da

NOME DO LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
				política VC não encontrada

VDA multissessão

Os seguintes eventos são registrados no log de eventos da máquina VDA multissessão:

NOME DO LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
Sistema	13	`Rpm`	Informação	O canal virtual personalizado `<vcName>` foi aberto pelo processo `<processName>`
Sistema	14	`Rpm`	Aviso	O canal virtual personalizado `<vcName>` não pode ser aberto pelo processo `<processName>`
Sistema	15	`Rpm`	Informação	`<username>` abriu o canal virtual personalizado `<vcName>`
Sistema	16	`Rpm`	Aviso	`<username>` tentou abrir o canal virtual personalizado `<vcName>`
Sistema	17	`Rpm`	Erro	O caminho fornecido na política

NOME DO LOG	ID	ORIGEM	NÍVEL	DESCRIÇÃO
				`<pathInPolicy>` não pode ser resolvido para o caminho do processo
Sistema	18	`Rpm`	Informação	O caminho do processo carregado é `<processPath>`
Sistema	19	`Rpm`	Erro	Variável de ambiente `<varName>` no caminho da política VC não foi encontrada

Canais virtuais de terceiros conhecidos

A seguir estão soluções de terceiros conhecidas que usam canais virtuais Citrix® personalizados. Esta lista não inclui todas as soluções que usam um canal virtual Citrix personalizado.

- Cerner
- ControlUp
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop Software
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Microsoft Teams
- Midmark IQPath Client Extensions
- Nuance PowerMic Client Extensions
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings para VDI

- Ultima IA-Connect

Para obter detalhes sobre como adicionar os canais virtuais associados à lista de permissões, entre em contato com os fornecedores das soluções. Alternativamente, siga as etapas descritas na seção Obtenção de nomes e processos de canais virtuais.

Lista de Permissão de Canal Virtual para DVC

Você pode usar a lista de permissão de canal virtual para DVC para controlar quais canais virtuais dinâmicos personalizados são permitidos em seu ambiente. Por padrão, nenhum canal virtual dinâmico é permitido. Se houver necessidade de canais virtuais dinâmicos, eles precisam ser explicitamente adicionados à lista de permissão.

Configuração

A lista de permissão de canal virtual para DVC é habilitada por padrão. Você pode configurar esse recurso usando a seguinte configuração na política Citrix®:

- Lista de permissão de canal virtual para DVC: para habilitar ou desabilitar o recurso e adicionar canais virtuais dinâmicos à lista.
- Limitação de log da lista de permissão de canal virtual: define o período de limitação para o registro de eventos da lista de permissão de canal virtual.
- Registro em log da lista de permissão de canal virtual: define o nível de registro em log para a lista de permissão de canal virtual.

Adicionando canais virtuais dinâmicos à lista de permissão

Para adicionar um canal virtual dinâmico à lista de permissão, você precisa das seguintes informações:

1. O nome do plug-in DVC no cliente. Por exemplo, `DvcPlugin1.dll`.
2. O nome do(s) listener(s) DVC. Por exemplo, `ListenerName1`.
3. Os caminhos para os processos que acessam o canal virtual dinâmico na máquina VDA. Por exemplo, `C:\Program Files\Application\run.exe`.

Depois de ter as informações necessárias, você deve adicionar o canal virtual dinâmico à lista de permissão usando a configuração de política da lista Permissão de canal virtual para DVC. Para adicionar um canal virtual dinâmico à lista, insira o caminho para o processo que acessa o DVC no host da sessão seguido por uma vírgula, depois o nome do plug-in do lado do cliente seguido por uma vírgula e o nome do listener usado pelo plug-in. Vários nomes de listener podem ser adicionados separados por vírgulas.

Para um único listener

Usando os exemplos anteriores, adicione a seguinte entrada à lista: `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1`

Para múltiplos ouvintes

Se houver vários ouvintes, adicione a seguinte entrada à lista: `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1,ListenerName2`

Usando curingas

O uso de curingas (*) é suportado. Você pode usar curingas quando os nomes de diretórios ou executáveis mudam com base na versão do aplicativo, ou se o componente de terceiros estiver instalado nos perfis dos usuários.

Você pode usar curingas nos seguintes cenários:

- Para substituir o nome completo do diretório. Por exemplo: `C:\Program Files\App*\run1.exe`
- Para substituir parte do nome do diretório. Por exemplo: `C:\Program Files\App\v*\run1.exe`
- Para substituir o nome do executável. Por exemplo: `C:\Program Files\App\v1.2*.exe`
- Para substituir parte do nome do executável. Por exemplo: `C:\Program Files\App\v1.2\run*.exe`

As seguintes restrições se aplicam:

- O curinga só pode ser usado para substituir um único diretório. Por exemplo, se o executável estiver localizado em `C:\Program Files\App\v1.2\run1.exe`
  - Permitido: `C:\Program Files\App*\run1.exe`
  - Não permitido: `C:\Program Files*\run1.exe`
- As entradas devem conter a extensão do nome do arquivo.
  - Permitido: `C:\Program Files\App\v1.2*.exe`
  - Não permitido: `C:\Program Files\App\v1.2*`
- Todos os caminhos devem ser locais.

Dispositivos

O HDX™ oferece uma experiência de usuário de alta definição em qualquer dispositivo, em qualquer local. Os artigos na seção Dispositivos descrevem estes dispositivos:

- Mapeamento de Unidade Cliente
- Dispositivo USB genérico
- Dispositivos móveis e de tela sensível ao toque
- Dispositivos seriais
- Teclados especiais
- Dispositivos TWAIN
- Webcams
- Dispositivos WIA

Dispositivo USB otimizado vs. genérico

Um dispositivo USB otimizado é aquele para o qual o aplicativo Citrix Workspace™ tem suporte específico. Por exemplo, a capacidade de redirecionar webcams usando o canal virtual HDX Multimedia. Um dispositivo genérico é um dispositivo USB para o qual não há suporte específico no aplicativo Citrix Workspace.

Por padrão, o redirecionamento USB genérico não pode redirecionar dispositivos USB com suporte a canal virtual otimizado, a menos que sejam colocados no modo Genérico.

Em geral, você obtém melhor desempenho para dispositivos USB no modo Otimizado do que no modo Genérico. No entanto, há casos em que um dispositivo USB não possui funcionalidade completa no modo Otimizado. Pode ser necessário mudar para o modo Genérico para obter acesso total aos seus recursos.

Com dispositivos de armazenamento em massa USB, você pode usar o mapeamento de unidade cliente ou o redirecionamento USB genérico, ou ambos, controlados por políticas Citrix®. As principais diferenças são:

Se as políticas de redirecionamento USB genérico e de mapeamento de unidade cliente estiverem habilitadas e um dispositivo de armazenamento em massa for inserido antes ou depois do início de uma sessão, ele será redirecionado usando o mapeamento de unidade cliente.

Quando estas condições são verdadeiras, o dispositivo de armazenamento em massa é redirecionado usando o redirecionamento USB genérico:

- Ambas as políticas de redirecionamento USB genérico e de mapeamento de unidade cliente estão habilitadas.
- Um dispositivo está configurado para redirecionamento automático.
- Um dispositivo de armazenamento em massa é inserido antes ou depois do início de uma sessão.

Para obter mais informações, consulte Configurar o redirecionamento automático de dispositivos USB.

RECURSO	MAPEAMENTO DE UNIDADE CLIENTE	REDIRECIONAMENTO USB GENÉRICO
Habilitado por padrão	Sim	Não
Acesso somente leitura configurável	Sim	Não
Acesso a dispositivo criptografado	Sim, se a criptografia for desbloqueada antes que o dispositivo seja acessado na sessão virtual.	Somente Citrix Virtual Desktops™

Mapeamento de Unidade Cliente (CDM)

O Mapeamento de Unidade Cliente disponibiliza unidades de armazenamento no endpoint do cliente dentro de uma sessão Citrix HDX™ para permitir que arquivos e pastas sejam transferidos do cliente para o host da sessão e vice-versa. Este recurso é habilitado por padrão com privilégios de leitura e gravação. Para impedir que os usuários adicionem ou alterem arquivos e pastas em dispositivos cliente mapeados, habilite a configuração de política **Acesso somente leitura à unidade cliente**. Ao adicionar esta configuração a uma política, certifique-se de que a configuração **Redirecionamento de unidade cliente** esteja definida como **Permitido** e também seja adicionada à política.

Como precaução de segurança, as unidades de endpoint são mapeadas sem a permissão de execução por padrão. Para permitir que os usuários executem arquivos executáveis diretamente das unidades cliente mapeadas, edite o valor do registro **ExecuteFromMappedDrive** no host da sessão. Para obter detalhes, consulte Unidades cliente mapeadas na seção **Recursos HDX gerenciados através do registro**.

Requisitos

A seguir estão os requisitos para usar o CDM:

Plano de controle Citrix

- Citrix Virtual Apps and Desktops™ 1912 ou posterior
- Citrix DaaS™

Host da sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows Server 2016 ou posterior
  - Linux: Consulte os requisitos de sistema do Linux VDA
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 ou posterior
  - Linux: Consulte a documentação do VDA para Linux

Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Linux: Consulte os requisitos de sistema do aplicativo Workspace para Linux

Políticas Relacionadas

Consulte a seção Referência de configurações de política para as configurações de CDM.

Cenários de salto duplo

O CDM é compatível em cenários de salto duplo. Por padrão, a unidade do endpoint do cliente é mapeada para a sessão do segundo salto e as unidades do primeiro salto não estão disponíveis. No entanto, isso pode ser configurado para que as unidades do primeiro salto sejam mapeadas na sessão do segundo salto, em vez das unidades do endpoint do cliente.

Para configurar a funcionalidade, edite o seguinte valor de registro:

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- Nome do valor: NativeDriveMapping
- Tipo de valor: REG_SZ
- Dados do valor:
  - True - Mapeia as unidades da sessão do primeiro salto na sessão do segundo salto
  - Falso - Mapeia as unidades do endpoint do cliente na sessão de segundo salto

> **Nota:**
>
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Dispositivos móveis e com tela sensível ao toque

O Citrix Virtual Apps and Desktops™ permite que os usuários acessem seus aplicativos e desktops publicados a partir de dispositivos cliente móveis e com tela sensível ao toque.

Requisitos

Plano de controle Citrix®

- Citrix Virtual Apps and Desktops 7.15 ou posterior
- Citrix DaaS™

Host de sessão

- Sistema operacional
  - Windows 10 1903 ou posterior
  - Windows Server 2016 ou posterior
- VDA
  - Windows: versão 7.15 ou posterior

Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
- Citrix Workspace™ app para Windows versão 1808 ou superior

Modo tablet para dispositivos com tela sensível ao toque usando o Windows Continuum

Continuum é um recurso do Windows 10 que se adapta à forma como o dispositivo cliente é usado. Quando o VDA detecta a presença de um teclado ou mouse em um cliente habilitado para toque, ele coloca o cliente no modo desktop. Se um teclado ou mouse não estiver presente, o VDA coloca o cliente no modo tablet/móvel. Essa detecção ocorre na conexão e reconexão da sessão e também durante a sessão quando o teclado ou mouse é conectado ou desconectado.

O recurso é habilitado por padrão. Para desabilitar este recurso, configure as configurações de política Configurações de política de alternância do modo tablet.

Além dos requisitos para dispositivos com tela sensível ao toque mencionados acima, os seguintes são necessários para o Windows Continuum:

XenServer®

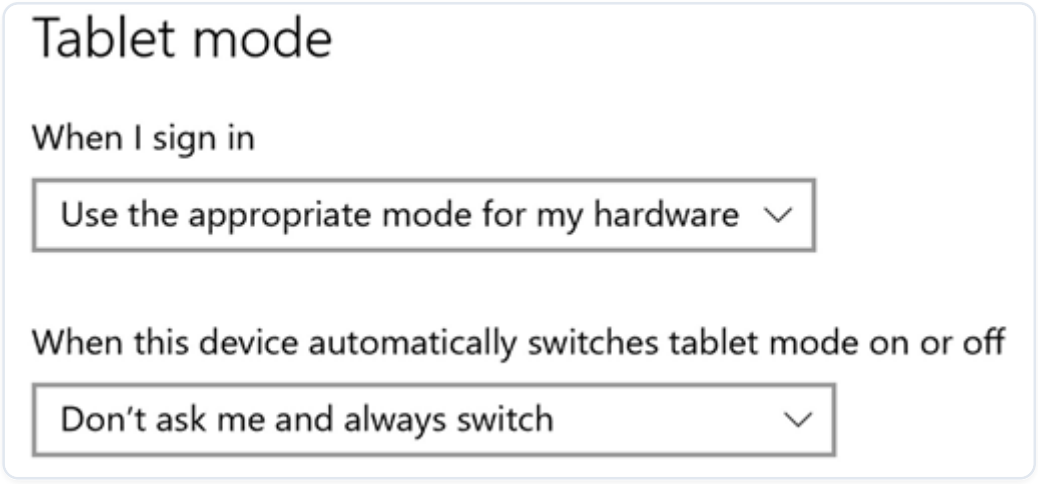
- Citrix Hypervisor 8.2 ou superior
- Execute o comando CLI do XenServer para permitir a alternância entre laptop/tablet: **xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1**

> **Importante:**

> A atualização da imagem base para um catálogo de máquinas existente após a alteração da configuração de metadados não afeta nenhuma VM provisionada anteriormente. Após alterar a imagem base da VM do XenServer, crie um catálogo, escolha a imagem base e provisione uma nova máquina do Machine Creation Services™ (MCS).

Host de sessão

- Sistema operacional
  - Windows 10 1903 ou posterior
  - Windows 11
- VDA
  - Windows: versão 7.16 ou posterior
  - **Devido às limitações atuais nas configurações do sistema operacional, o usuário terá que definir as seguintes opções nos menus suspensos depois de iniciar a primeira sessão ICA® e reiniciar o VDA:**
    - **Configurações > Sistema > Modo Tablet**
      - Usar o modo apropriado para meu hardware
      - Não me perguntar e sempre alternar



O **modo tablet** oferece uma interface de usuário mais adequada para telas sensíveis ao toque:

- Botões ligeiramente maiores
- A tela Iniciar e quaisquer aplicativos que você iniciar abrem em tela cheia
- A Barra de Tarefas contém um botão Voltar

- Ícones excluídos da barra de tarefas

Você tem acesso ao Explorador de Arquivos.



O Windows 10 carrega o driver GPIO na máquina virtual de destino com base neste BIOS atualizado. Ele é usado para alternar entre os modos tablet e desktop dentro da máquina virtual.

O aplicativo Citrix Workspace para HTML5 não oferece suporte aos recursos do Windows Continuum.

O **modo desktop** oferece a interface de usuário tradicional onde você interage da mesma forma que usaria um PC com teclado e mouse.

Canetas Microsoft Surface Pro e Surface Book

Oferecemos suporte à funcionalidade padrão da caneta com aplicativos baseados em Windows Ink. O suporte inclui apontar, apagar, pressão da caneta, sinais Bluetooth e outros recursos, dependendo do firmware do sistema operacional e do modelo da caneta. Por exemplo, a pressão da caneta pode ter até 4096 níveis. Este recurso é ativado por padrão.

A seguir estão os requisitos para o suporte à funcionalidade da caneta:

Plano de controle Citrix

- Citrix Virtual Apps and Desktops 1903 ou posterior
- Citrix DaaS

Host de sessão

- Sistema operacional

    - Windows 10 1809 ou posterior
    - Windows Server 2016 ou posterior
    - Windows 11
- VDA
    - Windows: versão 1903 ou posterior

Dispositivo cliente

- Sistema operacional
    - Windows 10 1809 ou posterior
- Aplicativo Citrix Workspace para Windows versão mínima 1902

Para uma demonstração do Windows Ink e da funcionalidade da caneta, clique nesta imagem:



Para desabilitar ou habilitar esse recurso, consulte Canetas Microsoft Surface Pro e Surface Book na lista de recursos gerenciados pelo registro.

Problemas conhecidos

A seguir estão os problemas conhecidos com o suporte à caneta:

- Devido a limitações do sistema operacional no Windows Server 2k22, os usuários não conseguirão definir atalhos de caneta ou fazer ajustes nas configurações de caneta/tinta no Painel de Controle ao se conectar a aplicativos ou desktops do servidor 2k22.
- Os atalhos de caneta não estão sendo respeitados de um cliente Windows 11 habilitado para caneta devido a uma limitação do sistema operacional.

Dispositivos seriais

A maioria dos PCs novos não possui portas seriais (COM) integradas. As portas são fáceis de adicionar usando conversores USB. Aplicativos adequados para portas seriais geralmente envolvem sensores, controladores, leitores de cheque antigos, pads e assim por diante. Alguns dispositivos USB de porta COM virtual usam drivers específicos do fornecedor em vez dos drivers fornecidos pelo Windows (usbser.sys). Esses drivers permitem que você force a porta COM virtual do dispositivo USB para que ela não mude mesmo se conectada a diferentes soquetes USB. Isso

pode ser feito em **Gerenciador de Dispositivos > Portas (COM e LPT) > Propriedades** ou no aplicativo que controla o dispositivo.

O mapeamento de porta COM do cliente permite que dispositivos conectados às portas COM no endpoint do usuário sejam usados durante sessões virtuais. Você pode usar esses mapeamentos como qualquer outro mapeamento de rede.

Para cada porta COM, um driver no sistema operacional atribui um nome de link simbólico, como COM1 e COM2. Os aplicativos então usam o link para acessar a porta.

> **Importante:**

> O fato de um dispositivo poder ser conectado ao endpoint usando USB diretamente não significa que ele possa ser redirecionado usando o redirecionamento USB genérico. Alguns dispositivos USB funcionam como portas COM virtuais, que os aplicativos podem acessar da mesma forma que uma porta serial física. O sistema operacional pode abstrair portas COM e tratá-las como compartilhamentos de arquivos. Dois protocolos comuns para COM virtual são CDC ACM ou MCT. Quando conectados por meio de uma porta RS-485, os aplicativos podem não funcionar. Obtenha um conversor RS-485 para RS232 para usar RS-485 como uma porta COM. **Importante:**

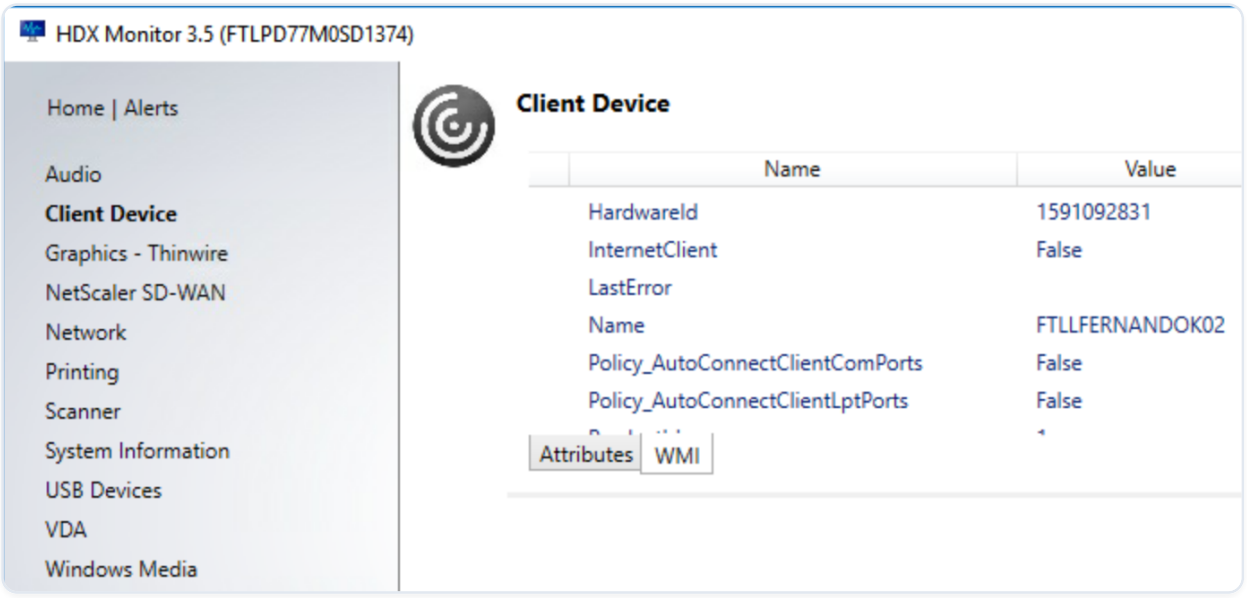
> Alguns aplicativos reconhecem o dispositivo (por exemplo, um pad de assinatura) de forma consistente apenas se ele estiver conectado a COM1 ou COM2 na estação de trabalho cliente.

Mapear uma porta COM do cliente para uma porta COM do servidor

Você pode mapear portas COM do cliente para uma sessão Citrix® de três maneiras:

- Políticas do Studio. Para obter mais informações sobre políticas, consulte Configurações de política de redirecionamento de porta.
- Prompt de comando do VDA.
- Ferramenta de configuração da Área de Trabalho Remota (Serviços de Terminal).

1. Habilite as políticas **Redirecionamento de porta COM do cliente** e **Conectar automaticamente portas COM do cliente do Studio**. Após aplicadas, algumas informações estarão disponíveis no HDX™ Monitor.



2. Se a **Conexão automática de portas COM do cliente** falhou ao mapear a porta, você pode mapear a porta manualmente ou usar scripts de logon. Faça logon no VDA e, em uma janela de prompt de comando, digite:

   NET USE COMX: \\\CLIENT\COMZ:

   Ou

   NET USE COMX: \\\CLIENT\\CLIENTPORT:COMZ:

   X é o número da porta COM no VDA (as portas de 1 a 9 estão disponíveis para mapeamento). **Z** é o número da porta COM do cliente que você deseja mapear.

   Para confirmar que a operação foi bem-sucedida, digite **NET USE** em um prompt de comando do VDA. A lista que aparece contém unidades mapeadas, portas LPT e portas COM mapeadas.

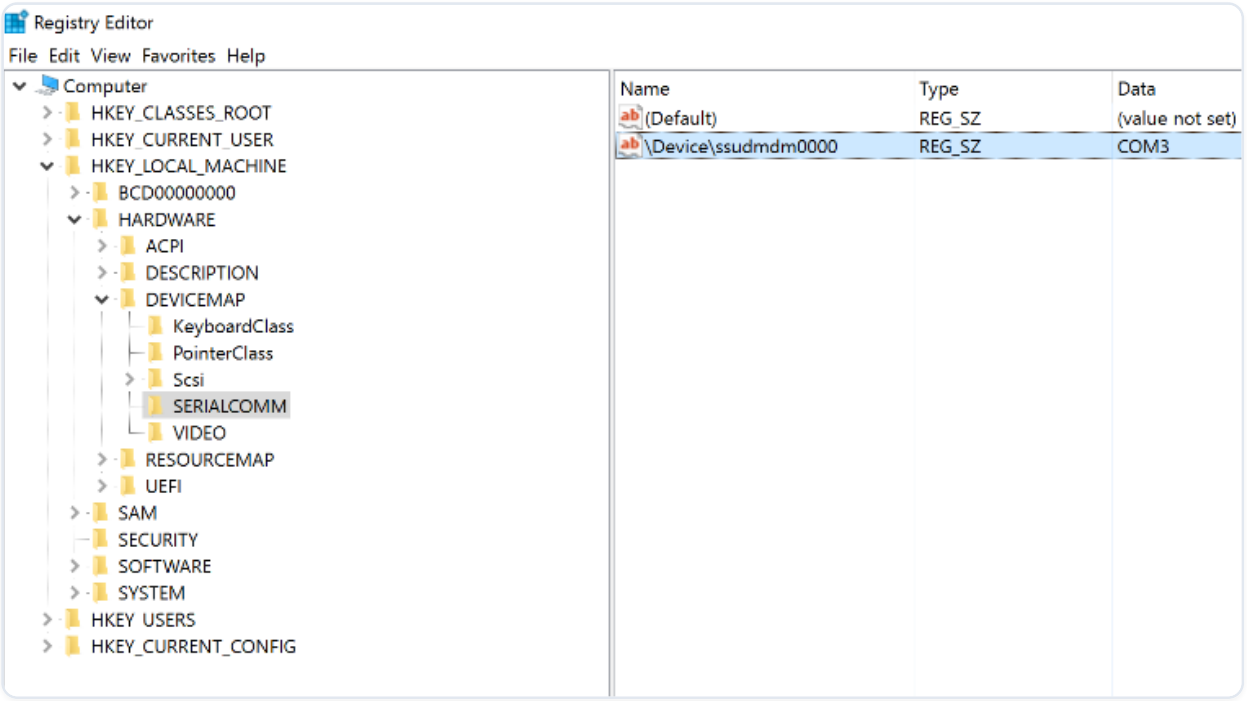


3. Para usar esta porta COM em um desktop ou aplicativo virtual, instale o aplicativo do seu dispositivo de usuário e aponte-o para o nome da porta COM mapeada. Por exemplo, se você mapear COM1 no cliente para COM3 no servidor, instale o aplicativo do seu dispositivo de porta COM no VDA e aponte-o para COM3 durante a sessão. Use esta porta COM mapeada como usaria uma porta COM no dispositivo do usuário.

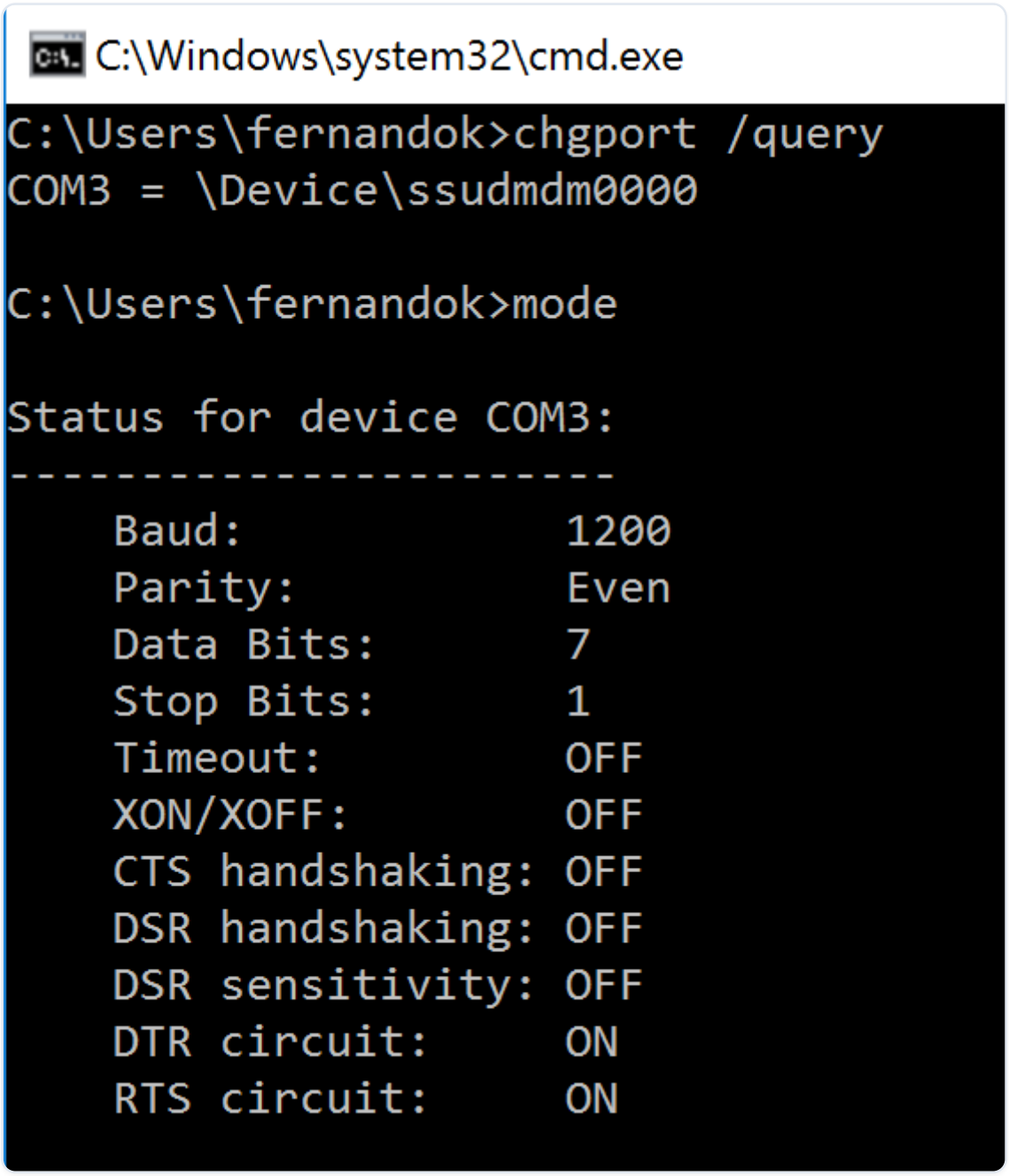
> **Importante:**
>
> O mapeamento de porta COM não é compatível com TAPI. Você não pode mapear dispositivos da Interface de Programação de Aplicativos de Telefonia do Windows (TAPI) para portas COM do cliente. TAPI define uma maneira padrão para os aplicativos controlarem as funções de telefone para chamadas de dados, fax e voz. TAPI gerencia a sinalização, incluindo discagem, atendimento e encerramento de chamadas. Além disso, serviços suplementares como retenção, transferência e chamadas em conferência.

Solução de problemas

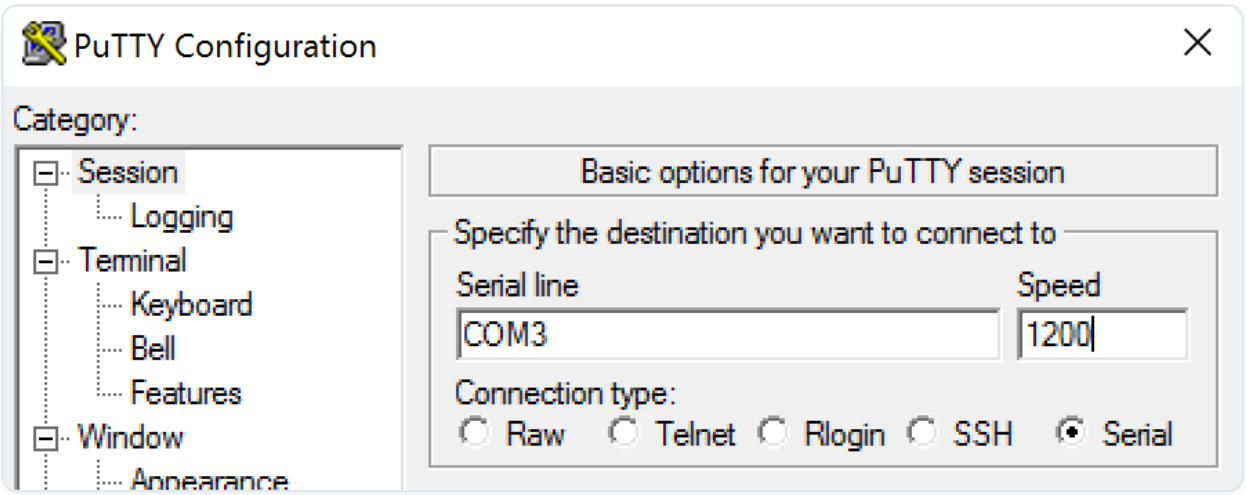
1. Certifique-se de que você pode acessar o dispositivo diretamente do endpoint, ignorando o Citrix. Enquanto a porta não estiver mapeada para o VDA, você não estará conectado a uma sessão Citrix. Siga todas as instruções de solução de problemas que vieram com o dispositivo e verifique se ele funciona localmente primeiro. Quando um dispositivo é conectado a uma porta COM serial, uma chave de registro é criada no hive mostrado aqui:



   Você também pode encontrar essas informações no prompt de comando executando **chgport /query**.



Se as instruções de solução de problemas para o dispositivo não estiverem disponíveis, tente abrir uma sessão PuTTY. Escolha **Session** e em **Serial line** especifique sua porta COM.



Você pode executar **MODE** em uma janela de comando local. A saída pode exibir a porta COM em uso e os valores de Baud/Paridade/Bits de Dados/Bits de Parada, que você precisa em sua sessão PuTTY. Se a conexão PuTTY for bem-sucedida, pressione **Enter** para ver o feedback do dispositivo. Quaisquer caracteres que você digitar podem ser repetidos na tela ou respondidos. Se esta etapa não for bem-sucedida, você não poderá acessar o dispositivo a partir de uma sessão virtual.

2. Mapeie a porta COM local para o VDA (usando políticas ou **NET USE COMX: \\ \CLIENT\COMZ:**) e repita os mesmos procedimentos do PuTTY da etapa anterior, mas desta vez a partir do PuTTY do VDA. Se o PuTTY falhar ao exibir o erro **Unable to open connection to COM1. Unable to open serial port**, outro dispositivo pode estar usando a COM1.
3. Execute **chgport /query**. Se o driver serial integrado do Windows no VDA estiver atribuindo automaticamente \Device\Serial0 a uma porta COM1 do seu VDA, faça o seguinte: A. Abra o CMD no VDA e digite **NET USE.**

   B. Exclua qualquer mapeamento existente (por exemplo, COM1) no VDA.

   NET USE COM1 /DELETE

   C. Mapeie o dispositivo para o VDA.

   NET USE COM1: \\\CLIENT\COM3:

   D. Aponte seu aplicativo no VDA para COM3.

   Por fim, tente mapear sua porta COM local (por exemplo, COM3) para uma porta COM diferente no VDA (que não seja COM1, por exemplo, COM3). Certifique-se de que seu aplicativo esteja apontando para ela: **NET USE COM3: \\\CLIENT\COM3**
4. Se agora você vir a porta mapeada, o PuTTY estiver funcionando, mas nenhum dado estiver sendo transmitido, pode ser uma condição de corrida. O aplicativo pode se conectar e abrir a porta antes que ela seja mapeada, impedindo que seja mapeada. Tente uma das seguintes opções:

   - Abra um segundo aplicativo publicado no mesmo servidor. Aguarde alguns segundos para que a porta seja mapeada e, em seguida, abra o aplicativo real que tenta usar a porta.
   - Habilite as políticas de redirecionamento de porta COM no Editor de Política de Grupo no Active Directory em vez do Studio. Essas políticas são **Redirecionamento de porta COM do cliente** e **Conectar automaticamente portas COM do cliente**. As políticas aplicadas dessa forma podem ser processadas antes das políticas do Studio, garantindo que a porta

COM seja mapeada. As políticas Citrix são enviadas para o VDA e armazenadas em: `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

- Use este script de logon para o usuário ou, em vez de publicar o aplicativo, publique um script .bat que primeiro exclui qualquer mapeamento no VDA, mapeia novamente a porta COM virtual e, em seguida, inicia o aplicativo:

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: \\ \CLIENT\COM1: NET USE COM2: \\\CLIENT\COM2: MODE COM1: BAUD=1200 (ou qualquer valor necessário) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (ou qualquer valor necessário) START C:\\Program Files\\\<Your Software Path>\\\<your_software.exe>

5. O Process Monitor da Sysinternals é a ferramenta de último recurso. Ao executar a ferramenta no VDA, localize e filtre objetos como COM3, picaser.sys, CdmRedirector, mas especialmente \<your_app\>.exe. Quaisquer erros podem aparecer como Acesso Negado ou similar.

Teclados especializados

Teclados Bloomberg

> **Aviso:**
>
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

> O Citrix Virtual Apps and Desktops™ oferece suporte ao teclado Bloomberg modelo 4 Starboard (e ao modelo 3 anterior). Este teclado permite que clientes do setor financeiro usem os recursos especiais do teclado para acessar dados do mercado financeiro e realizar negociações rapidamente.

Este teclado é compatível com as caixas de comutação KVM e pode funcionar em dois modos:

- PC (Um cabo USB sem KVM)
- Modo KVM (Dois cabos USB, um roteado através do KVM)

> **Importante:**

> Recomendamos que você use o teclado Bloomberg com apenas uma sessão. Não recomendamos o uso do teclado com várias sessões simultâneas (um cliente para várias sessões).

> O teclado Bloomberg 4 é um dispositivo composto USB compreendendo quatro dispositivos USB em um único invólucro físico:

- Teclado.
- Leitor de impressão digital.
- Dispositivo de áudio com teclas para aumentar e diminuir o volume e silenciar o alto-falante e o microfone. Este dispositivo inclui alto-falante, microfone e conector para microfone e fone de ouvido integrados.
- Hub USB para conectar todos esses dispositivos ao sistema.

Requisitos:

- A sessão à qual o aplicativo Citrix Workspace™ para Windows está se conectando deve oferecer suporte a dispositivos USB.
- Mínimo do aplicativo Citrix Workspace 1808 para Windows ou Citrix Receiver para Windows 4.8 para oferecer suporte aos modelos 3 e 4 de teclado Bloomberg.
- Mínimo do aplicativo Citrix Workspace 1808 para Windows ou Citrix Receiver para Windows 4.12 para usar o modo KVM (dois cabos USB, um roteado através do KVM) para o Modelo 4.

Para obter informações sobre como configurar teclados Bloomberg no aplicativo Citrix Workspace para Windows, consulte Configurando teclados Bloomberg.

Para habilitar o suporte a teclado Bloomberg, consulte Teclados Bloomberg na lista de recursos gerenciados por meio do registro.

Verificar suporte:

Para determinar se o suporte a teclado Bloomberg está habilitado no aplicativo Citrix Workspace, verifique se o Desktop Viewer relata corretamente os dispositivos do teclado Bloomberg.

Cenário de área de trabalho:

Abra o Desktop Viewer. Se o suporte para teclado Bloomberg estiver habilitado, o Desktop Viewer mostra três dispositivos sob o ícone USB:

- Leitor de Impressão Digital Bloomberg

- Recursos do Teclado Bloomberg
- Bloomberg LP Keyboard 2013

Cenário somente de aplicativo contínuo:

Abra o menu **Connection Center** no ícone da área de notificação do aplicativo Citrix Workspace. Se o suporte para o teclado Bloomberg estiver habilitado, os três dispositivos aparecerão no menu **Devices**.

A marca de seleção ao lado de cada um desses dispositivos indica que eles são remotos para a sessão.

Webcams

Streaming de webcam de alta definição

Webcams podem ser usadas por aplicativos de videoconferência em execução na sessão virtual. O aplicativo no servidor seleciona o formato e a resolução da webcam com base nos tipos de formato suportados. Quando uma sessão é iniciada, o cliente envia as informações da webcam para o servidor. Escolha uma webcam no aplicativo de videoconferência. Quando a webcam e o aplicativo suportam renderização de alta definição, o aplicativo usa resolução de alta definição. Suportamos resoluções de webcam de até 1920x1080.

Este recurso requer o Citrix Receiver para Windows, versão mínima 4.10. Para uma lista de plataformas do aplicativo Citrix Workspace que suportam o redirecionamento de webcam HDX, consulte Matriz de recursos do aplicativo Citrix Workspace.

Para obter mais informações sobre streaming de webcam de alta definição, consulte Videoconferência HDX e compactação de vídeo de webcam.

Você pode usar uma chave de registro para desabilitar e habilitar o recurso e, em seguida, configurar uma resolução específica. Para obter informações, consulte Streaming de webcam de alta definição e Resolução de webcam de alta definição na lista de recursos gerenciados através do registro.

Digitalização

Um scanner é um dispositivo que digitaliza opticamente imagens, texto impresso, caligrafia ou um objeto e os converte em uma imagem digital.

Se você estiver usando um scanner e seu computador estiver executando o Windows, há uma boa chance de você estar usando o driver de scanner WIA. Este driver é responsável pela comunicação entre seu computador e o scanner.

- **Windows Image Acquisition** (WIA) é o modelo de driver e a interface de programação de aplicativos (API) da Microsoft que permite que o software se comunique com hardware de imagem, como scanners.
- **TWAIN** (Windows e Mac) é outro protocolo de digitalização que conecta scanners e aplicativos, fornecendo uma interface padrão. O TWAIN permite que os aplicativos adquiram imagens de dispositivos compatíveis com TWAIN (scanners, câmeras digitais, etc.).

Redirecionamento TWAIN

Introdução

TWAIN é um protocolo de digitalização usado para vincular software de imagem a scanners ou câmeras digitais.

Como o TWAIN funciona

- Digitalize seus documentos usando qualquer um dos aplicativos de 32 bits em sua sessão Citrix®.

> **Nota:**
>
> Use um scanner compatível com TWAIN conectado localmente para digitalizar os documentos.

- O módulo de digitalização Citrix redireciona a solicitação TWAIN para o scanner do cliente.
- Assim que a digitalização é concluída, o host da sessão é notificado.

Requisitos

Plano de Controle Citrix

- Citrix Virtual Apps and Desktops™ 1912 ou posterior
- Citrix DaaS™

Host da Sessão

- Sistema operacional

  - Windows 10 1809 ou posterior
  - Windows 11
  - Windows Server 2022 ou posterior
- VDA
  - Versão 1912 ou posterior
- Aplicativo
  - Aplicativo de 32 bits

Dispositivo Cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11
- Aplicativo Workspace
  - Windows: versão 1912 ou posterior
- Scanner
  - Scanner compatível com TWAIN

Configuração

- Instale os drivers TWAIN no endpoint do cliente.
- Configure dispositivos ou aplicativos para selecionar o protocolo de digitalização necessário, caso suportem TWAIN e WIA.
- Conecte o scanner ao endpoint do cliente localmente (via USB).
- Redirecione dispositivos TWAIN para a sessão via redirecionamento USB, se necessário.

> **Nota:**
>
> Dispositivos TWAIN não funcionam bem com o redirecionamento USB, resultando em baixa qualidade de digitalização.

Configurações de Política

Configurações de política para configurar o redirecionamento TWAIN e melhorar a digitalização.

- **Redirecionamento de dispositivo TWAIN do cliente:** para habilitar ou desabilitar o redirecionamento TWAIN.

  > **Nota:**
  >
  > Por padrão, o redirecionamento TWAIN está habilitado.

- **Nível de compactação TWAIN:** para definir os níveis de compactação para imagens do cliente para o host.

Para mais detalhes, consulte Configurações de política de dispositivos TWAIN.

Solução de Problemas

Experimente o TWAIN com o aplicativo de teste público Twacker, que pode ser baixado neste URL.

Siga as etapas para validar o TWAIN em uma sessão de desktop publicada:

1. Instale o **Twacker** no VDA.
2. Inicie o **Twacker** (versão de 32 bits).
3. Clique em **Arquivo > Selecionar Origem** e selecione seu scanner na lista.
4. Clique em **Arquivo > Adquirir**.
5. Clique no **botão Digitalizar** para testar seu scanner.

Se o **Twacker** conseguir digitalizar com sucesso, isso confirma que a configuração do **Citrix Virtual Apps and Desktops** está:

- Configurada para redirecionamento USB
- Usando dispositivos TWAIN
- Atendendo a todos os requisitos de dispositivo cliente local

Se você ainda tiver problemas de digitalização em um aplicativo específico, é provável que seja um problema de software.

Dispositivos WIA

Requisitos

- O scanner deve ser compatível com WIA.
- Instale os drivers WIA no dispositivo local. Eles não são necessários no servidor.
- Conecte o scanner localmente (por exemplo, via USB).
- Certifique-se de que o scanner esteja usando o serviço local do Windows Image Acquisition e não o driver TWAIN.
- Certifique-se de que nenhuma política seja aplicada à conta de usuário usada para o teste, e que esteja limitando a largura de banda dentro da sessão ICA®. Por exemplo, limite de largura de banda de redirecionamento USB do cliente.

Lista de permissões de aplicativos do Windows Image Acquisition

Uma lista de permissões permite controlar quais aplicativos no VDA podem acessar o redirecionamento de scanner do Windows Image Acquisition. O Editor do Registro usa a entrada da configuração da lista de permissões em cada VDA que contém o Windows Image Acquisition. Por padrão, nenhum aplicativo tem acesso ao Windows Image Acquisition.

Para ajustar o Windows Image Acquisition para aplicativos no VDA, consulte a configuração Lista de permissões de aplicativos do Windows Image Acquisition na lista de recursos gerenciados através do registro.

Para obter informações sobre as configurações de política, consulte Configurações de política de dispositivos WIA.

Dispositivos USB

A tecnologia HDX™ oferece **suporte otimizado** para a maioria dos dispositivos USB populares. Esses dispositivos incluem:

- Monitores
- Mouses
- Teclados
- Telefones de Voz sobre Protocolo de Internet
- Fones de ouvido
- Webcams

- Scanners
- Câmeras
- Impressoras
- Unidades
- Leitores de cartão inteligente
- Mesas digitalizadoras
- Pads de assinatura

O suporte otimizado oferece uma experiência de usuário aprimorada com melhor desempenho e eficiência de largura de banda em uma WAN. O suporte otimizado geralmente é a melhor opção, especialmente em ambientes de alta latência ou sensíveis à segurança.

A tecnologia HDX fornece **redirecionamento USB genérico** para dispositivos especiais que não possuem suporte otimizado ou onde ele é inadequado. Para obter mais informações sobre o redirecionamento USB genérico, consulte Redirecionamento USB genérico.

Para obter mais informações sobre dispositivos USB e o aplicativo Citrix Workspace para Windows, consulte Configurando o redirecionamento de dispositivo USB composto e Configurando o suporte USB.

Configuração

O redirecionamento USB está desabilitado por padrão. Você pode configurar o redirecionamento USB genérico usando as seguintes configurações na política Citrix®:

- **Redirecionamento de dispositivo USB do cliente**: para habilitar ou desabilitar o redirecionamento USB
- **Regras de redirecionamento de dispositivo USB do cliente**: para especificar uma ação de dispositivo específica, ou seja, para permitir ou negar acesso a um dispositivo específico
- **Regras de redirecionamento de dispositivo USB do cliente (Versão 2)**: para especificar regras para filtrar, dividir e conectar automaticamente dispositivos USB
- **Regras de otimização de dispositivo USB do cliente**: para desabilitar a otimização ou alterar o modo de otimização
- **Permitir que dispositivos USB existentes sejam conectados automaticamente**: para permitir ou impedir a conexão automática de dispositivos USB existentes que estão conectados a um endpoint cliente no início de uma sessão HDX™

- **Permitir que dispositivos USB recém-chegados sejam detectados automaticamente**: para permitir ou impedir a conexão automática de dispositivos USB que estão conectados a um endpoint cliente durante uma sessão HDX

Consulte, Configurações de Política USB para mais detalhes.

Como configurar o redirecionamento USB

Por padrão, a configuração de redirecionamento USB está desabilitada. Para usá-lo, a política de redirecionamento USB e as regras de redirecionamento específicas devem ser habilitadas e configuradas no DDC.

> **Nota:**
>
> Se você estiver usando componentes anteriores à versão 2212 ou estiver usando o Workspace App para Linux/Mac, consulte Configuração de Redirecionamento USB Legado para obter detalhes sobre como configurar o redirecionamento USB.

Habilitando o Redirecionamento USB Genérico

1. Abra as **políticas do Citrix Web Studio™** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA® > Dispositivos USB**.
3. Edite a **política de redirecionamento de dispositivo USB do cliente**.
4. Selecione **Permitido** e clique em **Salvar**.

Criação de Regras de Política de Redirecionamento USB

Quando o usuário tenta redirecionar um dispositivo USB para o Virtual Desktop, ele é verificado em cada regra de política USB, uma por uma, até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada final. Se a primeira correspondência for uma regra de **Permitir**, o dispositivo correspondente pode ser redirecionado para o desktop virtual. Se a primeira correspondência for uma regra de **Negar**, o dispositivo correspondente estará disponível apenas no desktop local. Se nenhuma correspondência for encontrada, as regras padrão serão usadas.

REGRAS DE DISPOSITIVO

Assim como nos dispositivos USB regulares, as regras de dispositivo definidas na política ou na configuração do aplicativo Citrix Workspace™ do cliente no ponto de extremidade selecionam os

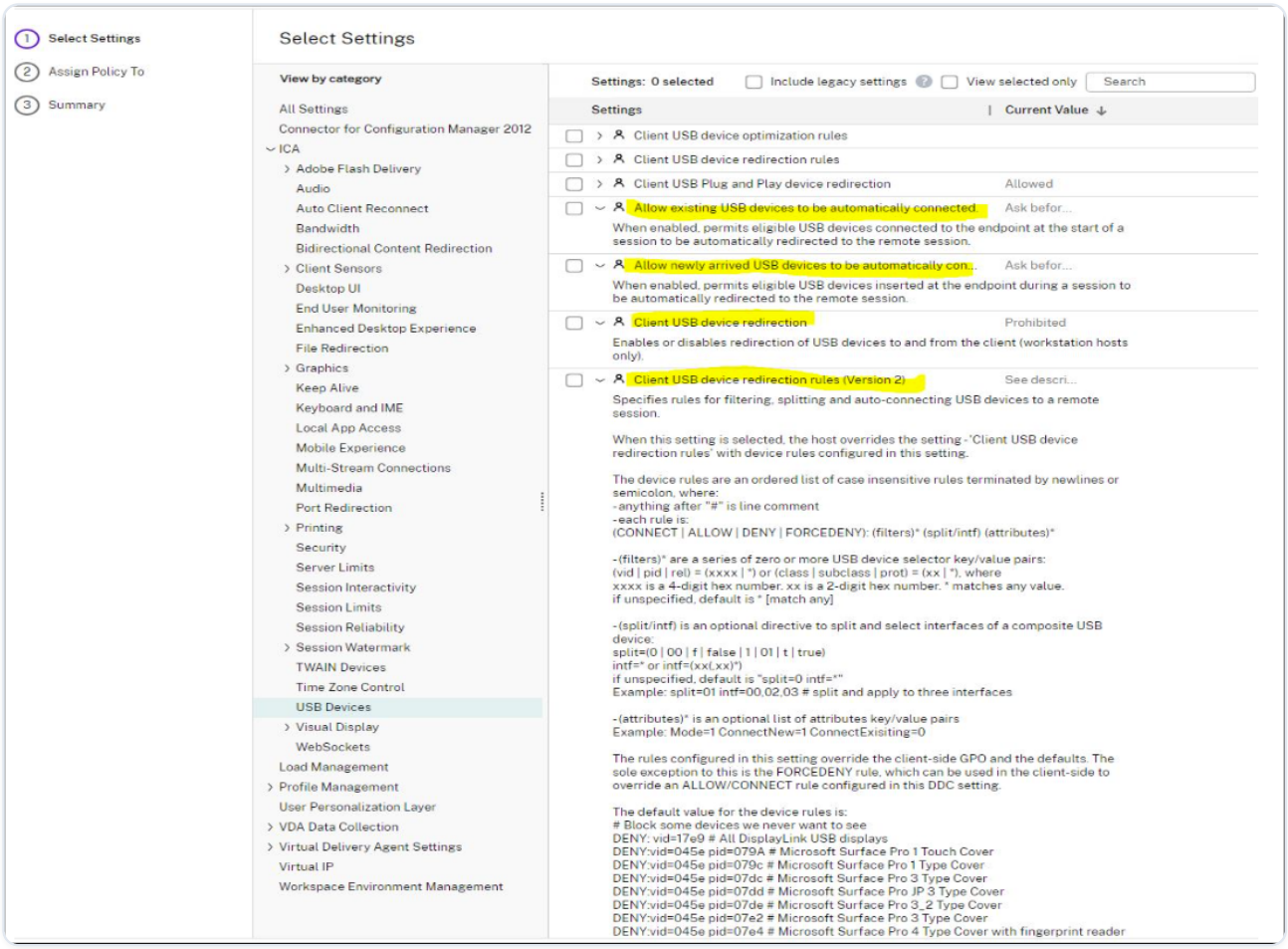
dispositivos para encaminhamento. O aplicativo Citrix Workspace usa essas regras para decidir quais dispositivos USB permitir ou impedir o encaminhamento para a sessão remota.

Cada regra consiste em uma palavra-chave de ação (**Permitir, Conectar ou Negar**), dois pontos (:) e zero ou mais parâmetros de filtro que correspondem aos dispositivos reais no subsistema USB dos endpoints. Esses parâmetros de filtro correspondem aos metadados do descritor de dispositivo USB usados por cada dispositivo USB para se identificar.

As regras de dispositivo são texto simples, com cada regra em uma única linha e um comentário opcional após um caractere #. As regras são correspondidas de cima para baixo (ordem de prioridade decrescente). A primeira regra que corresponde ao dispositivo ou interface filho é aplicada. As regras subsequentes que selecionam o mesmo dispositivo ou interface são ignoradas.

Exemplo: ALLOW VID=1050 PID=0421 #Device1 **Exemplo:** CONNECT VID=xxxx PID=yyyy Class=03 #Device2

PALAVRA-CHAVE	DESCRIÇÃO
CONNECT	Use esta palavra-chave para permitir que os dispositivos sejam redirecionados pelo canal virtual USB, bem como para habilitá-los para redirecionamento automático durante o início da sessão e na inserção.
ALLOW	Use este termo para permitir que dispositivos sejam redirecionados através do canal virtual USB
NEGAR	Use este termo para negar que dispositivos sejam redirecionados através do canal virtual USB



Configurando a política no DDC:

1. Abra as **políticas do Citrix Web Studio** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA > Dispositivos USB**.
3. Edite as **regras de redirecionamento de dispositivo USB do cliente** (**Versão 2**).
4. Defina o valor com base nos exemplos fornecidos na descrição para cada dispositivo USB que precisa ser redirecionado e clique em Salvar.

   Por exemplo: Permitir: VID=056A PID=00A4 #STU-430 Negar: Class=08 subclass=05 # Armazenamento em Massa

> **Nota:**

> Se um administrador Citrix marcar **Usar valor padrão** e clicar em **Salvar**, as regras padrão podem ser encontradas no seguinte registro no VDA.

> **Cuidado!**

> Consulte o Aviso Legal no final deste artigo antes de usar o Editor do Registro.

> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

Nota:

> As políticas ainda podem ser definidas no dispositivo cliente usando regras de dispositivo de política de grupo, mas isso não é mais necessário em versões mais recentes do CVAD e do CWA.

> Para configuração legada de dispositivos USB, consulte Configuração de Redirecionamento USB Legado.

Configurar o redirecionamento automático de dispositivos USB (Opcional)

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado. Além disso, as configurações de preferência do usuário USB são definidas para conectar automaticamente os dispositivos USB. Nem sempre é melhor redirecionar todos os dispositivos USB. Os usuários podem redirecionar explicitamente dispositivos da lista de dispositivos USB que não são redirecionados automaticamente. Para evitar que os dispositivos USB sejam listados ou redirecionados, use DeviceRules no endpoint do cliente ou na política DDC. Esta política pode ser definida no DDC, no cliente usando uma GPO, usando as Preferências do aplicativo Citrix Workspace ou a guia Conexões em CDViewer. Todos esses métodos são descritos abaixo:

Definindo a política no DDC:

Existem duas políticas no DDC que podem ser definidas para permitir o redirecionamento automático de dispositivos USB-

- Permitir que dispositivos USB existentes sejam conectados automaticamente
- Permitir que dispositivos USB recém-chegados sejam conectados automaticamente

a. Abra as **políticas do Citrix Web Studio** e clique na guia **Políticas**.

b. Clique em **Criar Política** e expanda as **políticas ICA > Dispositivos USB**.

c. Edite a configuração **Permitir** que dispositivos USB existentes sejam conectados automaticamente.

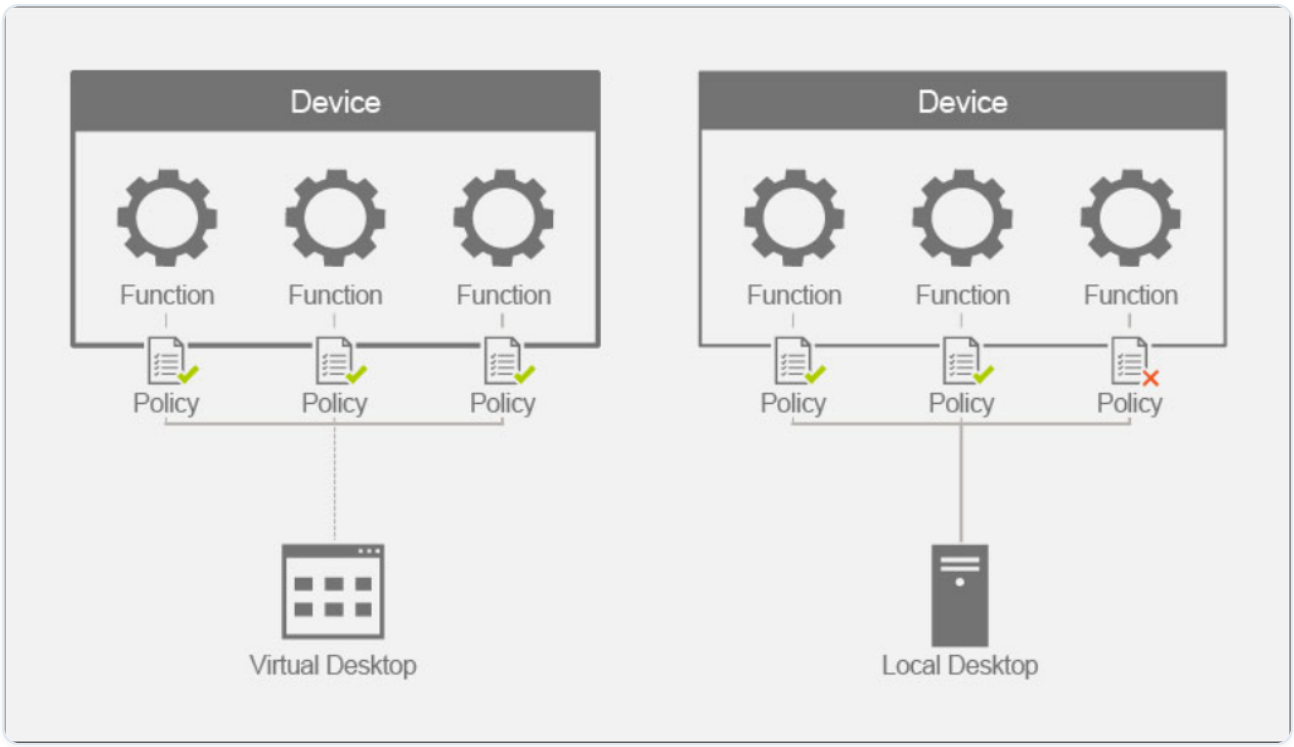
d. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

e. Edite a configuração **Permitir** que dispositivos USB recém-chegados sejam conectados automaticamente.

f. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Dispositivos Compostos e Divisão de Dispositivos

Um dispositivo USB composto é um único dispositivo que age como múltiplos dispositivos USB independentes conectados a um computador. Ele possui um único conector USB, mas pode expor múltiplas interfaces ao computador, cada uma com seu próprio conjunto de funcionalidades. Quando um usuário conecta um dispositivo USB composto, o dispositivo host verifica todas as funções (interfaces) em relação a cada regra de política. Se a primeira correspondência para qualquer função (interface) for uma regra de Negação, a regra é considerada definitiva para o dispositivo composto e o dispositivo é negado. Se a primeira correspondência para uma função (interface) for uma regra de Permissão, o dispositivo host continua a corresponder as regras à próxima função (interface). O dispositivo composto é permitido se nenhuma função (interface) for negada por uma regra de política. Se a correspondência definitiva para o dispositivo composto for uma Regra de Negação, o dispositivo estará disponível apenas para o desktop local; caso contrário, o dispositivo será redirecionado para o desktop virtual. Se nenhuma correspondência for encontrada, as regras padrão são usadas.



Podemos dividir o dispositivo composto usando as regras apropriadas na política de regras de redirecionamento de dispositivo (Versão 2) para permitir apenas funcionalidades específicas de um dispositivo composto. Por exemplo, podemos querer usar apenas as funções HID de uma chave FIDO2, mas não a funcionalidade de smartcard. Nesse caso, definiríamos as regras conforme ilustrado abaixo:

1. Conectar: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Funções HID FIDO2 permitidas da série 5 do Yubikey.
2. Negar: VID=1050 PID=0407 split=01 intf=02 # Função de smartcard da série 5 do Yubikey bloqueada.

> **Dica:**
>
> Ao criar novas regras de política, consulte os Códigos de Classe USB, disponíveis no site da USB.

Configurando uma mesa digitalizadora de assinatura

1. Instale o driver de dispositivo apropriado no host VDA.
2. Ative a **política de redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio™**.
3. Edite a política de **regras de redirecionamento de dispositivo USB do cliente** (**Versão 2**).
    a. Defina as informações de **VID** e **PID** para a mesa digitalizadora de assinatura que precisa ser redirecionada e clique em **Salvar**. Por exemplo: **Conectar**: VID=056A PID=00A4 #STU-430
4. Edite a política de **regras de otimização de dispositivo USB do cliente**.
    a. Defina o modo juntamente com outras informações do dispositivo. Por exemplo: Mode=00000004 VID=056A PID=00A4 class=03 #Dispositivo de entrada operando no modo de captura
5. Edite a política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

7. Edite a política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
8. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Uma vez que essas políticas são definidas no console do Studio, os lançamentos de sessão subsequentes terão o dispositivo sendo redirecionado automaticamente e não exigirão nenhuma ação adicional do usuário final.

> **Nota:**
>
> Substitua o VID e o PID pelos VID e PID reais do dispositivo a ser redirecionado.

Configurando o teclado Bloomberg usando redirecionamento USB

1. Ative a **política de redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
2. Os teclados Bloomberg 5 são definidos por padrão na política de regras de redirecionamento de dispositivo USB do cliente (Versão 2) e nenhuma ação administrativa adicional é necessária.
3. Edite a política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
4. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
5. Edite a política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Uma vez que essas políticas são definidas no console do Studio, as chaves Bloomberg serão apresentadas automaticamente nas sessões HDX™ subsequentes e não exigirão nenhuma ação adicional do usuário final.

Configurando uma chave FIDO2 usando redirecionamento USB

A Citrix recomenda usar o redirecionamento FIDO2 para usar chaves FIDO2 em suas sessões HDX. No entanto, pode haver situações em que você deve redirecionar chaves FIDO2 usando o redirecionamento USB. Isso inclui cenários em que o redirecionamento FIDO2 não está disponível

porque o recurso não é compatível com o cliente, o VDA ou o sistema operacional (por exemplo, Windows Server 2016).

Também pode haver situações em que a chave tem vários modos ativados, mas você deseja permitir apenas um subconjunto deles em suas sessões HDX. Por exemplo, você pode querer permitir FIDO2 e OTP, mas bloquear o cartão inteligente.

As etapas a seguir ilustram como você pode configurar uma chave FIDO2 usando o redirecionamento USB (Yubikey vid=1050, pid=0407).

1. Ative a **política de redirecionamento de dispositivo USB do cliente** no **Citrix Web Studio**.
2. Edite a política **Regras de redirecionamento de dispositivo USB do cliente** (Versão 2).
    a. Defina as informações de **VID** e **PID**, bem como a configuração de dispositivo dividido para a chave FIDO2 a ser redirecionada na sessão e clique em **Salvar**.
    b. **Conectar**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Funções HID FIDO2 permitidas da série 5 do Yubikey.
    c. **Negar**: VID=1050 PID=0407 split=01 intf=02 # Função de cartão inteligente da série 5 do Yubikey bloqueada.
3. Edite a política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
4. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
5. Edite a política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Uma vez que essas políticas são definidas no console do Studio, os teclados FIDO2 serão automaticamente apresentados em sessões HDX subsequentes e não exigirão nenhuma ação adicional do usuário final.

Configurando um mouse 3D usando redirecionamento USB

Atualmente, os drivers do mouse espacial 3dConnexion são suportados apenas em sistemas operacionais de estação de trabalho (Win 10 e Win11). Eles não funcionam em sistemas operacionais de servidor. A seguir estão as etapas para configurar um SpaceMouse Enterprise em um sistema operacional de estação de trabalho (vid=046D, pid=C016).

1. Instale o mais recente driver do Windows no host VDA.
2. No Studio, ative a **Política de redirecionamento de dispositivo USB do cliente**.
3. Edite a política **Regras de redirecionamento de dispositivo USB do cliente** (**Versão 2**).
    a. Defina as informações de **VID** e **PID** para o bloco de assinatura que precisa ser redirecionado e clique em **Salvar**. Por exemplo: **Conectar**: VID=046D PID=C016 #SpaceMouse Enterprise
4. Edite a política **Regras de otimização de dispositivo USB do cliente**.
    a. Defina o modo junto com outras informações do dispositivo. Por exemplo: Mode=00000004 VID=046D PID=C016 class=03 #Input device operating in capture mode
5. Edite a política **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente os dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
7. Edite a política **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
8. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente os dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Solução de problemas

As seguintes etapas devem ser seguidas para triar problemas relacionados ao redirecionamento USB:

1. Valide se os requisitos do sistema estão sendo atendidos para o redirecionamento USB. Isso inclui versões corretas de CVAD e CWA, dispositivos suportados e drivers de dispositivo na plataforma do sistema operacional em questão.
2. Certifique-se de que a configuração seja apropriada com base nas versões dos componentes e plataformas em uso no seu ambiente. Consulte a nota em Configuração de Redirecionamento USB Legado para obter detalhes sobre os componentes que exigem configurações de configuração legadas.
3. Valide se o dispositivo está listado entre os dispositivos que o cliente enumerou.
    a. Barra de ferramentas de Preferências do Workspace: Verifique os dispositivos enumerados na guia Dispositivos da barra de ferramentas de Preferências do aplicativo Workspace

(Clique com o botão direito do mouse no **ícone do CWA > Connection Center > Preferências**… Clique na guia **Dispositivos**).

b. `CtxUsbDiagnostics.exe` (Recomendado): Execute esta ferramenta em uma janela de prompt de comando. A saída fornece informações específicas do dispositivo para uma sessão específica. Ela informará se um dispositivo está sendo redirecionado ou não. Também informará se um conjunto de regras de dispositivo está impedindo o redirecionamento do dispositivo. Consulte Ferramenta de Diagnóstico para obter mais informações.

c. USBView ou outras ferramentas de terceiros: Execute uma ferramenta de terceiros como o USBView na máquina do endpoint/cliente para garantir que o dispositivo seja detectado no endpoint.

4. Se você vir o dispositivo sendo enumerado:

   a. Se você vir uma regra de Negação na saída da ferramenta CtxUsbDiagnostics para um dispositivo específico, verifique as políticas configuradas no Studio e certifique-se de que as regras estejam configuradas corretamente na política da Versão 2. Se a regra de negação não aparecer na política do Studio, verifique a política do lado do cliente e, finalmente, os padrões do lado do cliente nessa ordem para encontrar a regra de negação correspondente.

   b. Se não houver uma regra de negação na saída do CtxUsbDiagnostics, o CWA permitirá o redirecionamento do dispositivo marcando/clicando no botão apropriado na guia dispositivos da janela Preferências (Dispositivos > Gerenciar dispositivos). Um dispositivo, uma vez redirecionado, estará disponível na sessão. Isso pode ser verificado consultando o gerenciador de dispositivos / USBView ou aplicativo similar na sessão HDX.

5. Se você não vir o dispositivo sendo apresentado dentro da sessão:

   a. É possível que o driver de dispositivo correto não esteja instalado corretamente no host VDA. Certifique-se de que as versões mais recentes dos drivers de dispositivo estejam instaladas corretamente no host VDA. Alguns drivers de dispositivo não são suportados em máquinas de servidor de terminal, portanto, certifique-se de que este não seja o caso com o dispositivo que você está tentando redirecionar.

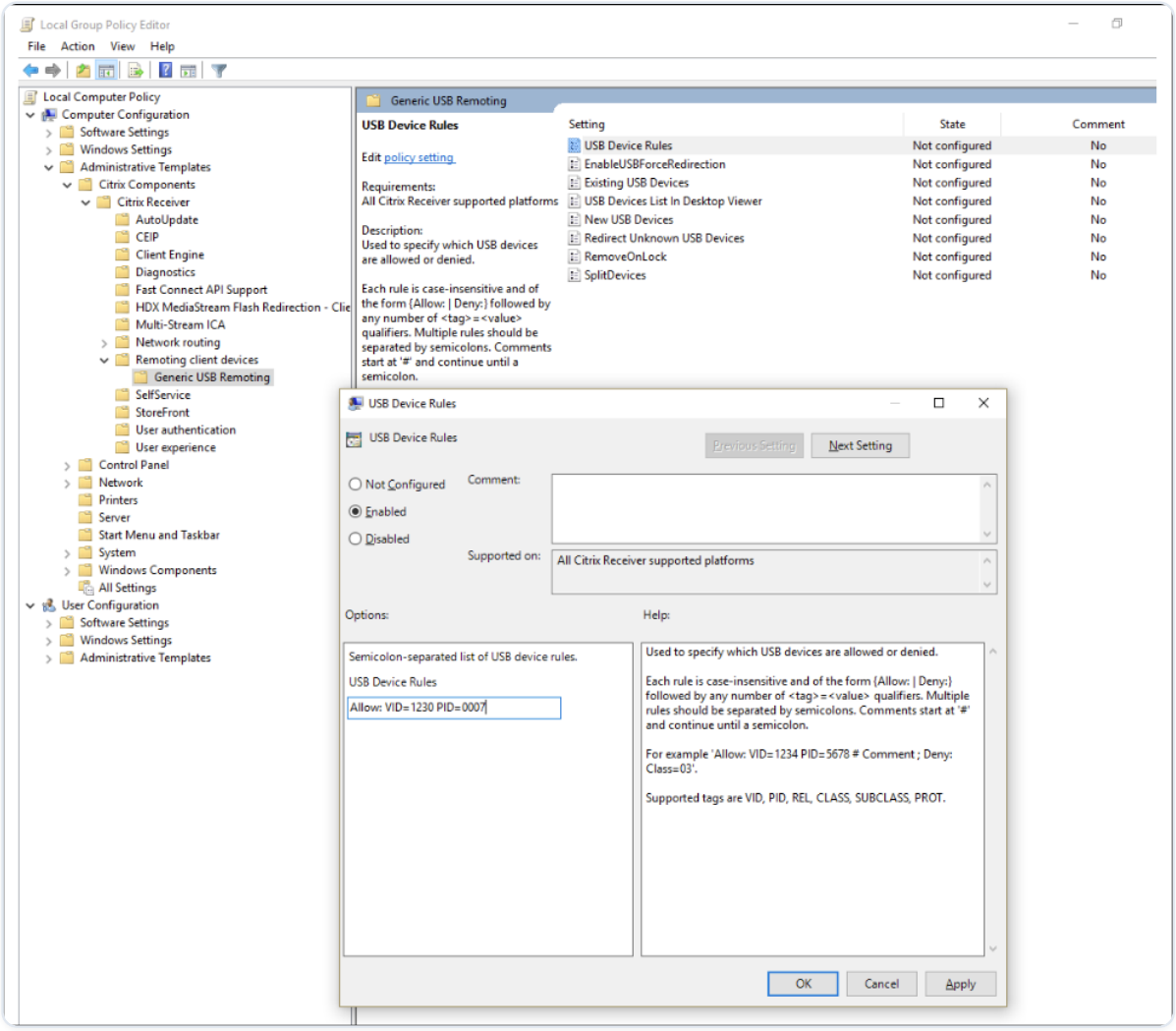
   b. Certifique-se de que o dispositivo não esteja sendo usado no endpoint do cliente. Alguns dispositivos exigem que os drivers sejam instalados também no endpoint do cliente, e isso pode impedi-los de serem redirecionados na sessão.

6. Valide se as regras relacionadas ao USB estão configuradas corretamente no endpoint do cliente:

a. **CWA para Windows** :

i. Valide se a política de grupo no cliente (adicione mais detalhes e capturas de tela para isso) está configurada corretamente e não entra em conflito com as regras definidas no Studio.

ii. Valide as regras padrão no registro do cliente.



`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`.

b. CWA para Linux - Para solucionar problemas do CWA para Linux, consulte a documentação USB para CWA para Linux

c. CWA para Mac - Para solucionar problemas do CWA para Mac, consulte CWA para Mac

Nota:

- No TSVDA, dispositivos de áudio são bloqueados por padrão de usar o redirecionamento USB. A maneira recomendada de usar esses dispositivos é usando o VC de Áudio otimizado.
- Às vezes, dispositivos compostos USB podem não ser divididos automaticamente, mesmo que uma regra de redirecionamento de dispositivo correta esteja definida para dividir o dispositivo. Esse problema ocorre porque o dispositivo está em modo de baixo consumo de energia. Nesses casos, o dispositivo filho que entra no modo de baixo consumo de energia pode não estar presente na lista de dispositivos. Você pode usar as seguintes soluções alternativas para superar esse problema:
  - Desconecte a sessão, insira o dispositivo USB e reconecte-se à sessão.
  - Desconecte o dispositivo USB e conecte-o novamente. Essa ação faz com que o dispositivo saia do modo de baixo consumo de energia.
- Às vezes, as configurações de economia de bateria USB podem ser ativadas para otimizar a vida útil da bateria. Se o endpoint do cliente entrar em suspensão, o dispositivo USB poderá ser desconectado. Nesse cenário, pode ser necessário desconectar e reconectar o dispositivo para apresentá-lo novamente na sessão.

Logs de Eventos

Os administradores agora podem monitorar dispositivos não autorizados que os usuários podem tentar redirecionar e tomar as ações apropriadas. Aqui estão algumas das mensagens de evento que serão registradas no Visualizador de Eventos no host VDA para dispositivos que podem ser redirecionados e para dispositivos que não podem.

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

Ferramenta de Diagnóstico USB

`CtxUsbDiagnostics.exe` é uma ferramenta de linha de comando no VDA para ajudar os administradores Citrix a diagnosticar e resolver problemas de redirecionamento de dispositivos USB experimentados no cliente de forma expedita. Esta ferramenta utilitária coleta informações vitais necessárias para triar problemas de configuração associados a dispositivos USB conectados ao cliente que não estão conseguindo redirecionar dentro de uma sessão HDX.

```
> **Note :**

>

> Running Command Prompt or Powershell as an administrator is required to
```

```
ensure the tool has the necessary permissions to perform system-level
operations.
```

Requisitos

Host de sessão

- Sistema operacional
  - Windows 10 1809 ou posterior
  - Windows 11 21H2 ou posterior
  - Windows Server 2016 ou posterior
- VDA
  - Windows: Citrix Virtual Apps and Desktops™ Versão 2311 ou posterior

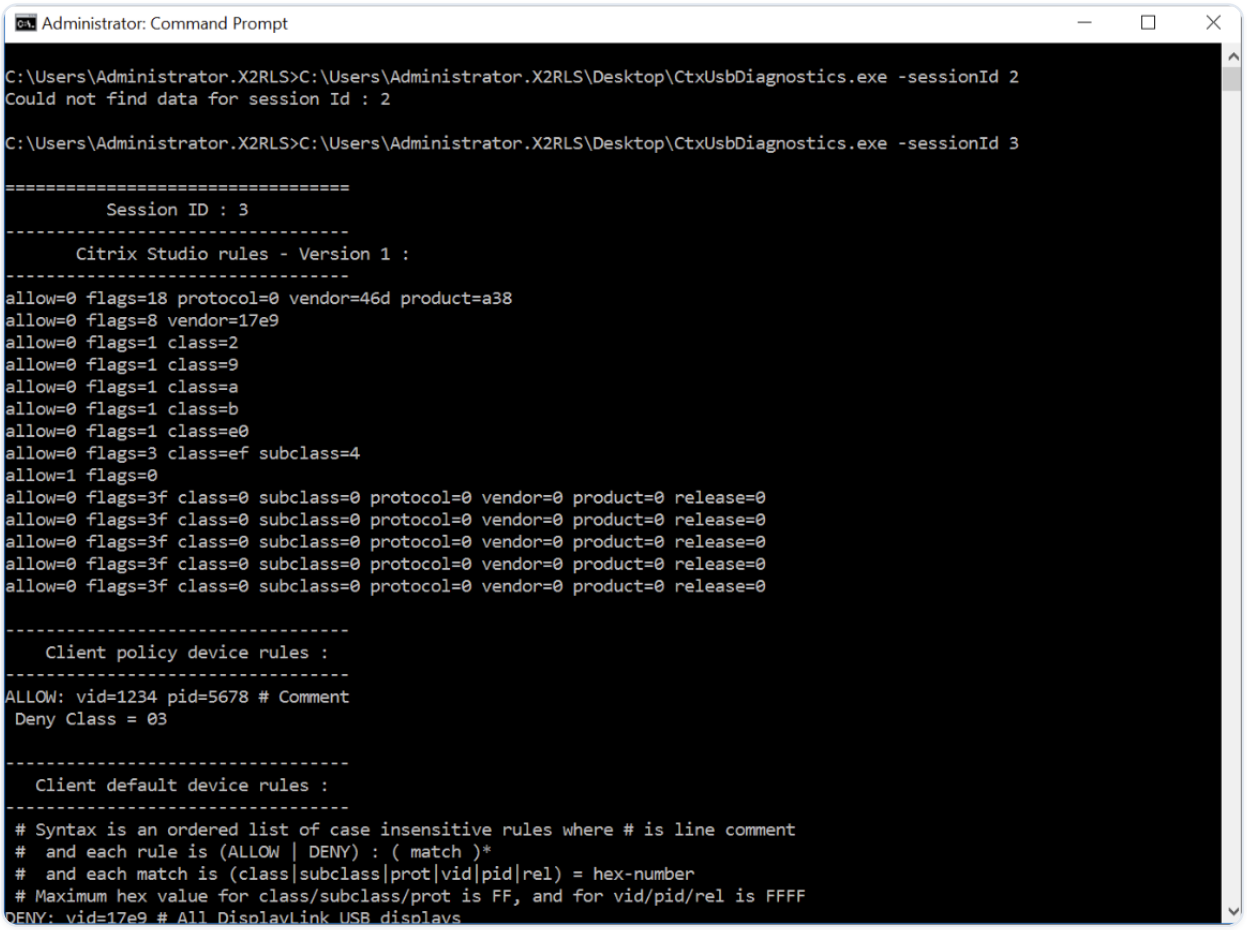
Dispositivo cliente

- Sistema operacional
  - Windows 10 1809 ou posterior
- Workspace App
  - Windows: versão 2311 ou posterior

O que a ferramenta faz?

A ferramenta atualmente fornece:

- SessionID
- Políticas de dispositivo VDA (regras de dispositivo definidas no Studio)
- Dispositivos cliente e políticas de dispositivo cliente (regras de dispositivo)
- Lista de dispositivos, seu estado de redirecionamento e por que foram permitidos ou negados



> **Nota :**
>
> O administrador pode ver as informações do dispositivo para todas as sessões ativas.

Informações Exibidas

- **Regras do Citrix Studio - Versão 1/2**
  - As regras DDC indicam o uso da política legada “**Client USB device redirection rules**” ou “**Client USB device redirection rules (Version 2)**” no Studio. As informações listadas nesta seção listam todas as regras configuradas pelo administrador Citrix®.

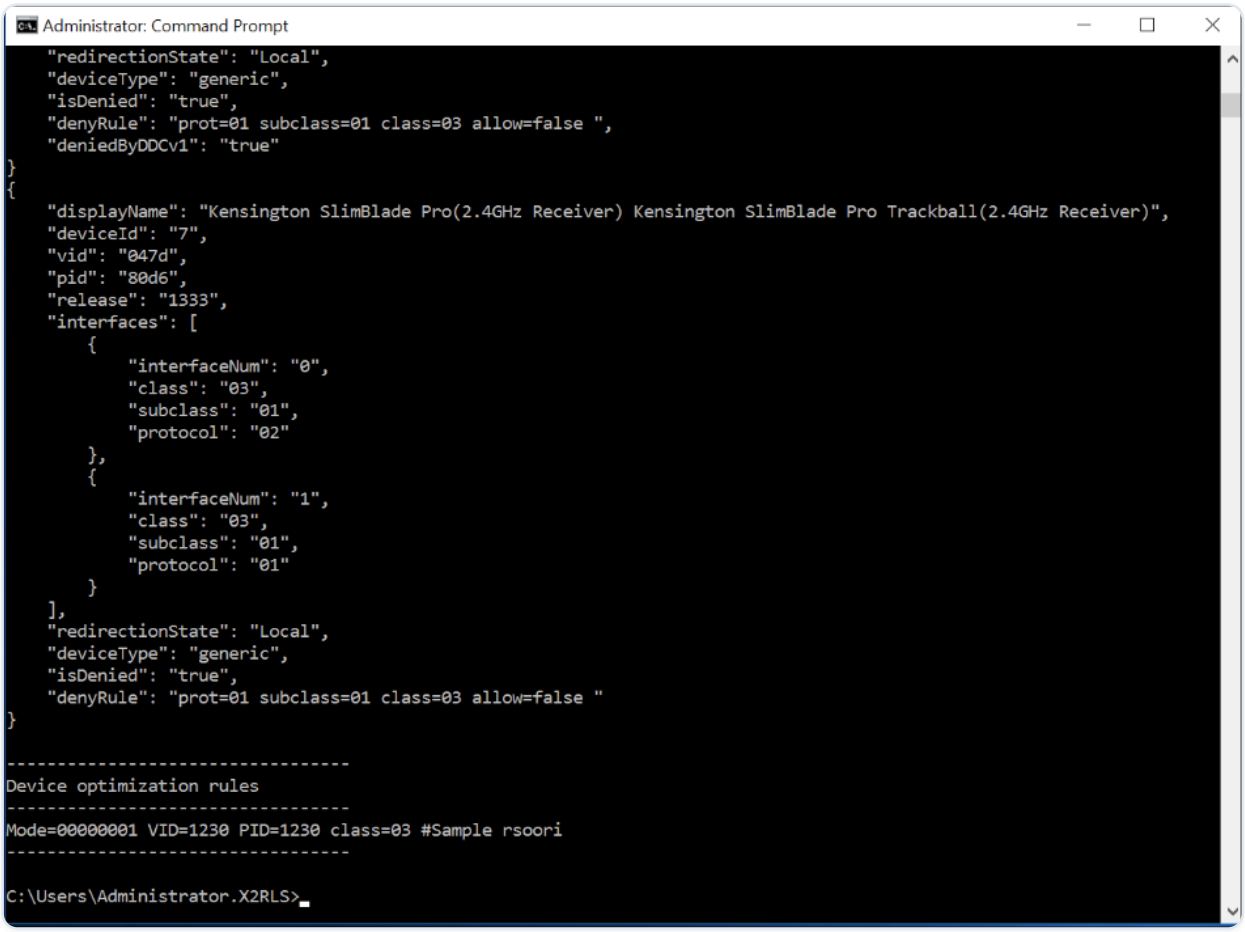
```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **Regras Padrão de Dispositivo Cliente**
  - Esta seção lista as regras que são definidas no registro no cliente.

```
---------------------------------
  Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #  and each rule is (ALLOW | DENY) : ( match )*
 #  and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **Regras de otimização de dispositivo**
  - Esta seção lista as regras de otimização de dispositivo conforme definido em "Regras de otimização de dispositivo USB do cliente".



Lista de Dispositivos

Esta seção lista informações valiosas sobre cada dispositivo conectado ao endpoint do cliente, as informações de hardware, se está sendo redirecionado ou não, se a regra de redirecionamento de dispositivo correta está definida ou não, e assim por diante.

NOME DA TAG	DESCRIÇÃO
displayName	Lista o nome comum do dispositivo.
ID do Fornecedor	ID do Fornecedor
ID do Produto	ID do Produto
Interfaces	Esta subseção lista todas as interfaces caso o dispositivo composto tenha sido dividido em vários dispositivos filhos.
Número da Interface	Indica o índice do descritor da interface
Classe	Código da classe

NOME DA TAG	DESCRIÇÃO
Subclasse	Código da subclasse
Protocolo	Protocolo
Estado de redirecionamento	**Local** indica que o dispositivo não é redirecionado na sessão ICA®. **EstaSessão** indica que o dispositivo é redirecionado na sessão ICA. **OutraSessão** indica que o dispositivo é redirecionado em outra sessão ICA.
Otimização ativada	**true** indica que o dispositivo está otimizado. **false** indica que o dispositivo não está otimizado e a transferência de dados ocorre através do canal virtual USB.
Tipo de dispositivo	**genérico** indica que o dispositivo não possui um canal virtual otimizado e o tráfego está fluindo através do canal virtual USB. **otimizado** implica que a transferência de dados associada ao dispositivo está ocorrendo através de um canal virtual dedicado.
isDenied	**true** indica que o dispositivo não é redirecionado devido a uma regra de política definida pelo administrador. `false` indica que o dispositivo é redirecionado devido à política aplicada.
denyRule	Este campo é útil se **isDenied** estiver definido como `true`. Ele informa ao administrador a regra específica definida na política que está resultando no não redirecionamento do dispositivo.

Configuração de Redirecionamento USB Legado

Se você estiver usando componentes anteriores à versão 2212 ou se estiver usando o CWA para Linux, siga este guia para configurar o redirecionamento USB em seu ambiente.

Habilitando o Redirecionamento USB Genérico

1. Abra as **políticas do Citrix Web Studio™** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA® > Dispositivos USB**.
3. Edite a **política de redirecionamento de dispositivo USB do cliente**.
4. Selecione **Permitido** e clique em **Salvar**.

Criando Regras de Política de Redirecionamento USB

Quando o usuário tenta redirecionar um dispositivo USB para o Virtual Desktop, ele é verificado em relação a cada regra de política USB, uma por uma, até que uma correspondência seja encontrada. A primeira correspondência para qualquer dispositivo é considerada final. Se a primeira correspondência for uma regra de Permissão, o dispositivo correspondente terá permissão para ser redirecionado para o desktop virtual. Se a primeira correspondência for uma regra de Negação, o dispositivo correspondente estará disponível apenas no desktop local. Se nenhuma correspondência for encontrada, as regras padrão serão usadas.

Configurando a política no DDC:

1. Abra as **políticas do Citrix Web Studio** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA > Dispositivos USB**.
3. Edite as **regras de redirecionamento de dispositivo USB do cliente**.
4. Defina o valor com base nos exemplos fornecidos na descrição para cada dispositivo USB que precisa ser redirecionado e clique em Salvar. Por exemplo: Permitir: VID=056A PID=00A4 #STU-430 Negar: Class=08 subclass=05 # Mass Storage

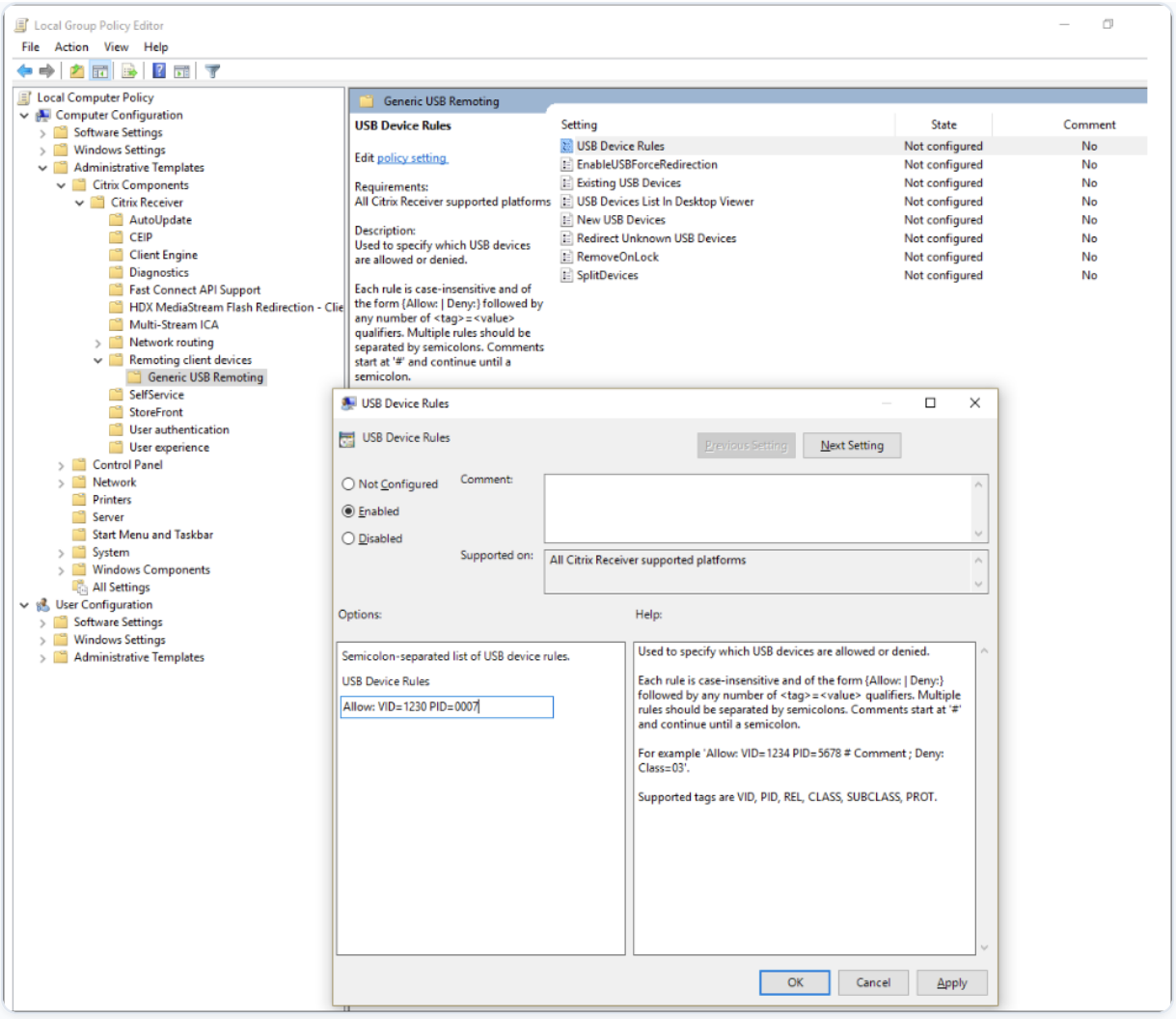
> **Nota:**
>
> Se um administrador Citrix® marcar Usar valor padrão e clicar em Salvar, as regras padrão podem ser encontradas no seguinte registro no VDA.
>
> **Cuidado!:**
>
> Consulte o Aviso Legal no final deste artigo antes de usar o Editor do Registro.
> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

Usando GPOs no cliente:

1. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver™ > Dispositivos de cliente de acesso remoto > Acesso Remoto USB Genérico**.
2. Abra a **configuração de Regras de Dispositivo USB** e ative a configuração. Adicione a regra de Dispositivo USB como neste exemplo, A regra Allow: VID=1230 PID=0007 permite o dispositivo com ID de Fornecedor 1230 e ID de Produto 0007.

Nota:

Use a regra Allow: VID=xxxx PID=xxxx quando um dispositivo específico deve estar no topo da lista de regras de dispositivo.



Nota:

> Uma ferramenta como USBView ou até mesmo a barra de ferramentas de Conexão pode ser usada para determinar os detalhes do dispositivo, como VID e PID (inclua SS aqui).

Configurar o redirecionamento automático de dispositivos USB

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado. Além disso, as configurações de preferência do usuário USB são definidas para conectar automaticamente os dispositivos USB. Nem sempre é melhor redirecionar todos os dispositivos USB. Os usuários podem redirecionar explicitamente dispositivos da lista de dispositivos USB que não são redirecionados automaticamente. Para evitar que os dispositivos USB sejam listados ou redirecionados, use DeviceRules no endpoint do cliente ou na política DDC.

Esta política pode ser definida no DDC, no cliente usando um GPO, usando as Preferências do Citrix Workspace™ app ou a guia Conexões em CDViewer. Todos esses métodos são descritos abaixo:

Definindo a política no DDC:

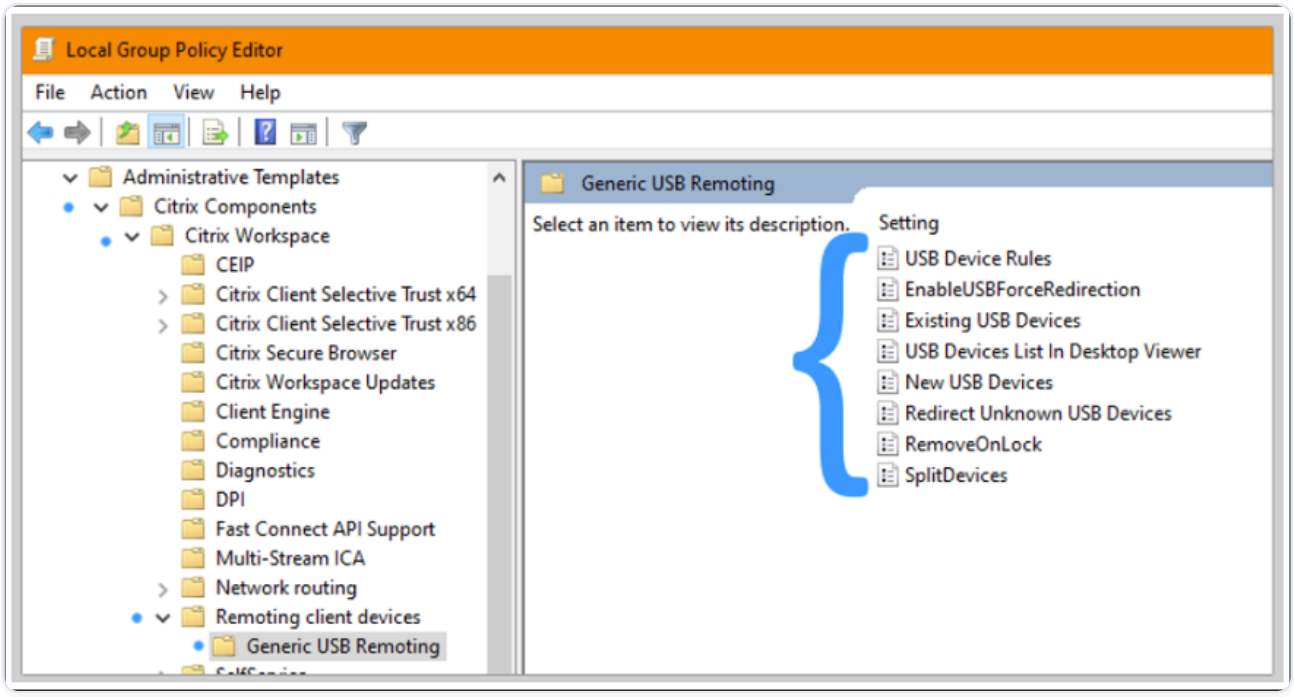
Existem duas políticas no DDC que podem ser configuradas para permitir o redirecionamento automático de dispositivos USB - “Permitir que dispositivos USB existentes sejam conectados automaticamente, Permitir que dispositivos USB recém-chegados sejam conectados automaticamente”

1. Abra as **políticas do Citrix Web Studio** e clique na guia **Políticas**.
2. Clique em **Criar Política** e expanda as **políticas ICA > Dispositivos USB**.
3. Edite a configuração **Permitir que dispositivos USB existentes sejam conectados automaticamente**.
4. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.
5. Edite a configuração **Permitir que dispositivos USB recém-chegados sejam conectados automaticamente**.
6. Desmarque a caixa de seleção **Usar valor padrão** e selecione **Redirecionar automaticamente dispositivos USB disponíveis** no menu suspenso e clique em **Salvar**.

Usando GPOs no cliente:

1. Abra o **Editor de Política de Grupo Local** e vá para **Modelos Administrativos > Componentes Citrix > Citrix Receiver > Dispositivos cliente de acesso remoto > Acesso remoto USB genérico**.

2. Abra **Novos Dispositivos USB**, selecione **Habilitado** e clique em **OK**.
3. Abra **Dispositivos USB Existentes**, selecione **Habilitado** e clique em **OK**.

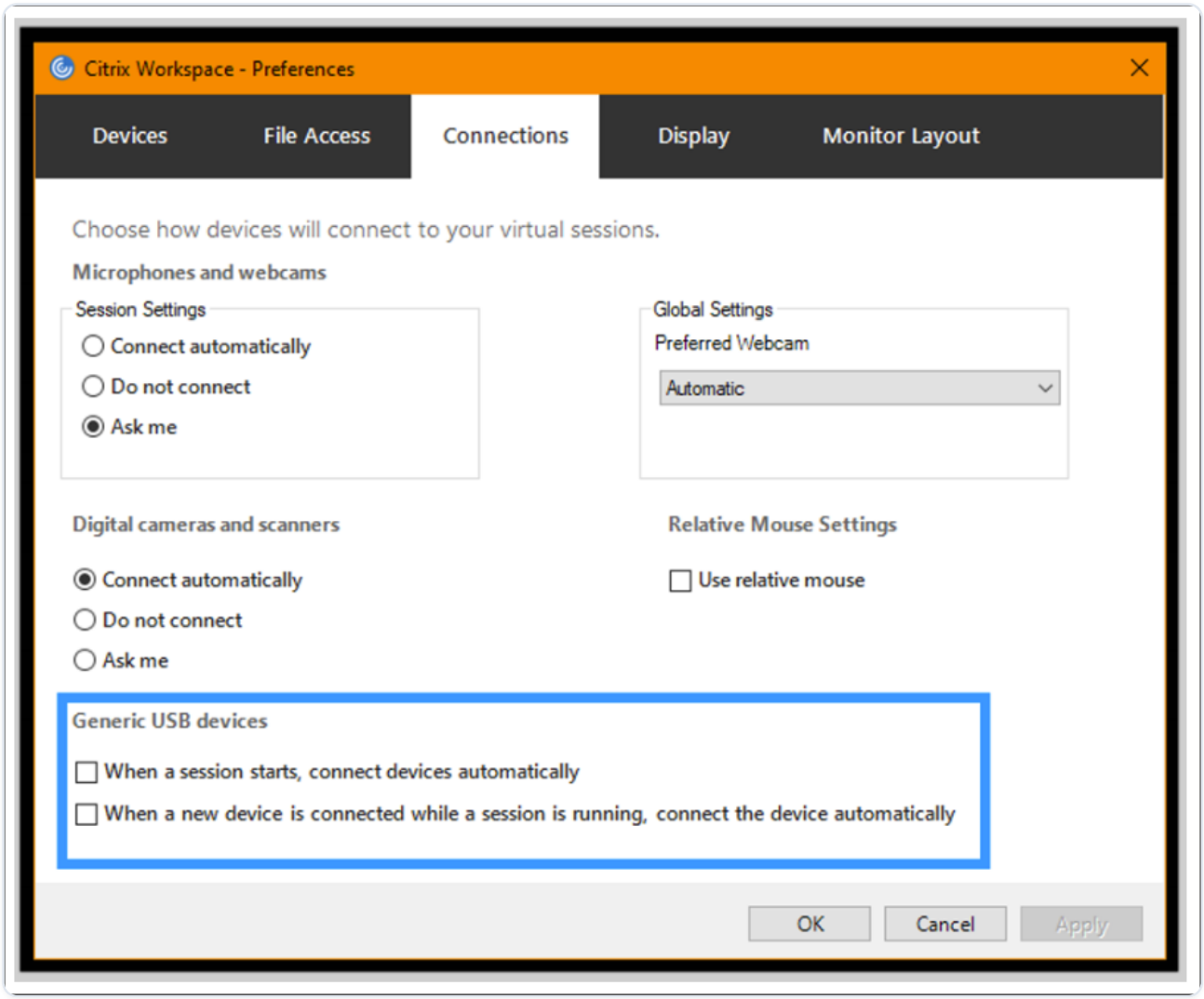


Usando o Citrix Connection Center:

1. Vá para **Preferências do Citrix Workspace > Conexões**.
2. Certifique-se de que as seguintes opções estejam selecionadas:
    a. Quando uma sessão é iniciada, conectar dispositivos automaticamente
    b. Quando um novo dispositivo é conectado enquanto uma sessão está em execução, conectar o dispositivo automaticamente.
3. Clique em **OK**.

Usando a barra de ferramentas de conexão do CDViewer:

1. Após o início de uma sessão, clique no menu suspenso **CDViewer** e selecione a guia **Citrix Workspace Preferences > Connections**.
2. Certifique-se de que as seguintes opções estejam selecionadas:
    a. Quando uma sessão é iniciada, conectar dispositivos automaticamente
    b. Quando um novo dispositivo é conectado enquanto uma sessão está em execução, conectar o dispositivo automaticamente.
3. Clique em **Aplicar** e **OK** para salvar a política.



Para as configurações baseadas no cliente, as chaves de registro são definidas no dispositivo cliente no seguinte local:

> **Cuidado!:**

> Consulte o Aviso Legal no final deste artigo antes de usar o Editor do Registro.
> `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

Gráficos

Os gráficos Citrix HDX incluem um extenso conjunto de tecnologias de aceleração e codificação de gráficos que otimizam a entrega de aplicativos gráficos avançados do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™). As tecnologias gráficas proporcionam a mesma experiência de usar um desktop físico ao trabalhar remotamente com aplicativos virtuais que são intensivos em gráficos.

Você pode usar software ou hardware para renderização de gráficos. A renderização por software requer uma biblioteca de terceiros chamada rasterizador de software. Por exemplo, o Windows inclui o rasterizador WARP para gráficos baseados em DirectX. Às vezes, você pode querer usar um renderizador de software alternativo. A renderização por hardware (aceleração de hardware) requer um processador gráfico (GPU).

O HDX™ Graphics oferece uma configuração de codificação padrão otimizada para os casos de uso mais comuns. Usando as políticas da Citrix, os administradores de TI também podem configurar várias definições relacionadas a gráficos para atender a diferentes requisitos e proporcionar a experiência de usuário desejada.

Thinwire

Thinwire é a tecnologia de exibição remota padrão da Citrix usada no Citrix DaaS.

A tecnologia de exibição remota permite que gráficos gerados em uma máquina sejam transmitidos, geralmente por uma rede, para outra máquina para exibição. Os gráficos são gerados como resultado da entrada do usuário, por exemplo, toques de tecla ou ações do mouse.

HDX 3D Pro

Os recursos do HDX 3D Pro no Citrix DaaS permitem que você entregue desktops e aplicativos que têm o melhor desempenho usando uma unidade de processamento gráfico (GPU) para aceleração de hardware. Esses aplicativos incluem aplicativos gráficos profissionais 3D baseados em OpenGL e DirectX. O VDA padrão suporta aceleração de GPU apenas para DirectX.

Aceleração de GPU para Windows Single-session OS

Ao usar o HDX 3D Pro, você pode entregar aplicativos graficamente intensivos como parte de desktops ou aplicativos hospedados em máquinas Single-session OS. O HDX 3D Pro suporta computadores host físicos (incluindo estações de trabalho desktop, blade e rack) e tecnologias de GPU Passthrough e virtualização de GPU oferecidas pelos hipervisores XenServer®, vSphere e Hyper-V (somente passthrough).

Usando o GPU Passthrough, você pode criar VMs que têm acesso exclusivo a hardware de processamento gráfico dedicado. Você pode instalar várias GPUs no hipervisor e atribuir VMs a cada uma dessas GPUs em uma base um-para-um.

Usando a virtualização de GPU, várias máquinas virtuais podem acessar diretamente o poder de processamento gráfico de uma única GPU física.

Aceleração de GPU para Windows Multi-session OS

O HDX 3D Pro permite que aplicativos com muitos gráficos em execução em sessões do Windows Multi-session OS sejam renderizados na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização de OpenGL, DirectX, Direct3D e Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não retarda a CPU do servidor. Além disso, o servidor é capaz de processar mais gráficos porque a carga de trabalho é dividida entre a CPU e a GPU.

Framehawk

> **Importante:**
>
> A partir do Citrix Virtual Apps and Desktops 7 1903, o Framehawk não é mais compatível. Em vez disso, use Thinwire com transporte adaptável ativado.

> Framehawk é uma tecnologia de acesso remoto de exibição para trabalhadores móveis em conexões sem fio de banda larga (redes celulares Wi-Fi e 4G/LTE). O Framehawk supera os desafios de interferência espectral e propagação multitrilha e oferece uma experiência de usuário fluida e interativa aos usuários de aplicativos e desktops virtuais.

Marca d'água de sessão baseada em texto

As marcas d'água de sessão baseadas em texto ajudam a impedir e permitem rastrear o roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um impedimento para aqueles que usam fotografias e capturas de tela para roubar dados. Você pode

especificar uma marca d'água que é uma camada de texto. A marca d'água pode ser exibida em toda a tela da sessão sem alterar o conteúdo do documento original. As marcas d'água de sessão baseadas em texto exigem suporte VDA.

Informações relacionadas

- HDX 3D Pro
- Aceleração de GPU para SO de sessão única do Windows
- Aceleração de GPU para SO de várias sessões do Windows
- Thinwire
- Marca d'água de sessão baseada em texto

HDX™ 3D Pro

Os recursos HDX 3D Pro do Citrix Virtual Apps and Desktops™ permitem que você forneça desktops e aplicativos que têm o melhor desempenho usando uma unidade de processamento gráfico (GPU) para aceleração de hardware. Esses aplicativos incluem aplicativos gráficos profissionais 3D baseados em OpenGL e DirectX. O VDA padrão suporta aceleração de GPU apenas para DirectX.

Para as configurações de política do HDX 3D Pro, consulte Otimizar para carga de trabalho de gráficos 3D.

Todos os aplicativos Citrix Workspace compatíveis podem ser usados com gráficos 3D. Para obter o melhor desempenho com cargas de trabalho 3D complexas, monitores de alta resolução, configurações de vários monitores e aplicativos de alta taxa de quadros, recomendamos as versões mais recentes do Citrix Workspace app para Windows e do Citrix Workspace app para Linux. Para obter mais informações sobre as versões compatíveis do Citrix Workspace app, consulte Marcos do ciclo de vida do Citrix Workspace app.

Exemplos de aplicativos profissionais 3D incluem:

- Aplicativos de design, fabricação e engenharia assistidos por computador (CAD/CAM/CAE)
- Software de Sistema de Informação Geográfica (GIS)
- Sistema de Comunicação e Arquivamento de Imagens (PACS) para imagens médicas
- Aplicativos que usam as versões mais recentes de OpenGL, DirectX, NVIDIA CUDA, OpenCL e WebGL

- Aplicativos não gráficos computacionalmente intensivos que usam GPUs NVIDIA Compute Unified Device Architecture (CUDA) para computação paralela

O HDX 3D Pro oferece a melhor experiência do usuário em qualquer largura de banda:

- Em conexões WAN: Ofereça uma experiência de usuário interativa em conexões WAN com larguras de banda tão baixas quanto 1,5 Mbps.
- Em conexões LAN: Ofereça uma experiência de usuário equivalente à de um desktop local em conexões LAN.

  Você pode substituir estações de trabalho complexas e caras por dispositivos de usuário mais simples, movendo o processamento gráfico para o data center para gerenciamento centralizado.

O HDX 3D Pro fornece aceleração de GPU para máquinas de SO de sessão única do Windows e máquinas de SO de várias sessões do Windows. Para obter mais informações, consulte Aceleração de GPU para SO de sessão única do Windows e Aceleração de GPU para SO de várias sessões do Windows.

O HDX 3D Pro é compatível com as tecnologias de passthrough de GPU e virtualização de GPU oferecidas pelos seguintes hypervisors, além de bare metal:

- XenServer®
  - Passthrough de GPU com NVIDIA GRID, AMD e Intel GVT-d
  - Virtualização de GPU com NVIDIA GRID, AMD e Intel GVT-g
  - Consulte a compatibilidade de hardware em Lista de Compatibilidade de Hardware do Hypervisor.

Use a ferramenta HDX Monitor para validar a operação e a configuração das tecnologias de visualização HDX e para diagnosticar e solucionar problemas do HDX. Para baixar a ferramenta e saber mais sobre ela, consulte `<https://taas.citrix.com/hdx/download/>`.

Aceleração de GPU para SO Windows multi-sessão

O HDX™ 3D Pro permite que aplicativos com uso intenso de gráficos executados em sessões do SO Windows Multi-sessão sejam renderizados na unidade de processamento gráfico (GPU) do servidor. Ao mover a renderização de OpenGL, DirectX, Direct3D e Windows Presentation Foundation (WPF) para a GPU do servidor, a renderização gráfica não retarda a CPU do servidor.

Além disso, o servidor é capaz de processar mais gráficos porque a carga de trabalho é dividida entre a CPU e a GPU.

Como o Windows Server é um sistema operacional multiusuário, vários usuários podem compartilhar uma GPU acessada pelo Citrix Virtual Apps™ sem a necessidade de virtualização de GPU (vGPU).

Para procedimentos que envolvem a edição do registro, use com cautela: A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Compartilhamento de GPU

O Compartilhamento de GPU permite a renderização de hardware de GPU de aplicativos OpenGL e DirectX em sessões de área de trabalho remota. Ele possui as seguintes características:

- Pode ser usado em máquinas bare metal ou virtuais para aumentar a escalabilidade e o desempenho do aplicativo.
- Permite que várias sessões simultâneas compartilhem recursos de GPU (a maioria dos usuários não exige o desempenho de renderização de uma GPU dedicada).
- Não requer configurações especiais.

Uma GPU pode ser atribuída à máquina virtual do Windows Server nos modos de passagem completa (full pass-through) ou GPU virtual (vGPU), seguindo os requisitos do Hypervisor e do fornecedor da GPU. Implantações bare-metal em máquinas físicas do Windows Server também são suportadas.

O Compartilhamento de GPU não depende de nenhuma placa gráfica específica.

- Para máquinas virtuais, selecione uma placa gráfica compatível com o Hypervisor em uso. Para uma lista de compatibilidade de hardware do XenServer, consulte Lista de Compatibilidade de Hardware do Hypervisor.
- Ao executar em bare metal, é recomendável ter um único adaptador de vídeo habilitado pelo sistema operacional. Se várias GPUs estiverem instaladas no hardware, desabilite todas, exceto uma, usando o Gerenciador de Dispositivos.

A escalabilidade usando o Compartilhamento de GPU depende de vários fatores:

- Os aplicativos em execução

- A quantidade de RAM de vídeo que eles consomem
- O poder de processamento da placa gráfica

Alguns aplicativos manipular a escassez de RAM de vídeo melhor do que outros. Se o hardware ficar sobrecarregado, pode ocorrer instabilidade ou uma falha do driver da placa gráfica. Limite o número de usuários simultâneos para evitar tais problemas.

Para confirmar que a aceleração da GPU está ocorrendo, use uma ferramenta de terceiros como o GPU-Z. O GPU-Z está disponível em `<http://www.techpowerup.com/gpuz/>`.

- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA e processadores gráficos Intel Iris Pro. Uma configuração de política (habilitada por padrão) controla esse recurso e permite o uso de codificação de hardware para codificação H.264 (onde disponível). Se tal hardware não estiver disponível, o VDA retorna à codificação baseada em CPU usando o codec de vídeo de software. Para mais informações, consulte Configurações de política de gráficos.

Renderização DirectX, Direct3D e WPF

A renderização DirectX, Direct3D e WPF está disponível apenas em servidores com uma GPU que suporta uma interface de driver de vídeo (DDI) versão 9ex, 10 ou 11.

- No Windows Server 2008 R2, DirectX e Direct3D não exigem configurações especiais para usar uma única GPU.
- No Windows Server 2012 e posterior, as sessões do Remote Desktop Services (RDS) no servidor RD Session Host usam o Microsoft Basic Render Driver como adaptador padrão. Para usar a GPU em sessões RDS no Windows Server 2012 e posterior, habilite a configuração **Usar o adaptador gráfico padrão de hardware para todas as sessões dos Serviços de Área de Trabalho Remota** na política de grupo **Política de Computador Local** \> **Configuração do Computador** \> **Modelos Administrativos** \> **Componentes do Windows** \> **Serviços de Área de Trabalho Remota** \> **Host da Sessão da Área de Trabalho Remota** \> **Ambiente de Sessão Remota**.
- Para permitir que aplicativos WPF renderizem usando a GPU do servidor, crie as configurações no registro do servidor que executa sessões do Windows Multi-session OS. Para obter informações sobre a configuração do registro, consulte Renderização do Windows Presentation Foundation (WPF) na lista de recursos gerenciados através do registro.

Aceleração de GPU para aplicativos CUDA ou OpenCL

A aceleração de GPU de aplicativos CUDA e OpenCL executados em uma sessão de usuário é desabilitada por padrão.

Para usar os recursos POC de aceleração CUDA, habilite as configurações do registro. Para obter informações, consulte Aceleração de GPU para aplicativos CUDA ou OpenCL na lista de recursos gerenciados através do registro.

Aceleração de GPU para SO de sessão única do Windows

Com o HDX 3D Pro, você pode fornecer aplicativos graficamente intensivos como parte de desktops hospedados ou aplicativos em máquinas de SO de sessão única. O HDX 3D Pro oferece suporte a computadores host físicos (incluindo estações de trabalho desktop, blade e rack) e tecnologias de Passthrough de GPU e virtualização de GPU oferecidas pelos hipervisores XenServer®, vSphere, Nutanix e Hyper-V (somente passthrough).

O HDX™ 3D Pro oferece os seguintes recursos:

- Compressão profunda adaptativa baseada em H.264 ou H.265 para desempenho ideal de WAN e sem fio. O HDX 3D Pro usa a compressão H.264 de tela cheia baseada em CPU como técnica de compressão padrão para codificação. A codificação de hardware com H.264 é usada com placas NVIDIA, Intel e AMD que suportam NVENC. A codificação de hardware com H.265 é usada com placas NVIDIA que suportam NVENC.
- Opção de compressão sem perdas para casos de uso especializados. O HDX 3D Pro também oferece um codec sem perdas baseado em CPU para suportar aplicativos onde gráficos perfeitos em pixels são necessários, como imagens médicas. A verdadeira compressão sem perdas é recomendada apenas para casos de uso especializados porque consome mais recursos de rede e processamento.

  Ao usar a compressão sem perdas:

  - O indicador sem perdas, um ícone na área de notificação, notifica o usuário se a tela exibida é um quadro com perdas ou um quadro sem perdas. Este ícone ajuda quando a configuração da política de **Qualidade Visual** especifica **Construir para sem perdas**. O indicador sem perdas fica verde quando os quadros enviados são sem perdas.
  - O switch sem perdas permite ao usuário mudar para o modo Sempre Sem Perdas a qualquer momento dentro da sessão. Para selecionar ou desmarcar **Sem perdas a qualquer momento dentro de uma sessão**, clique com o botão direito do mouse no ícone e clique em **Alternar para pixel perfeito** ou use o atalho ALT+SHIFT+1.

Para compressão sem perdas: O HDX 3D Pro usa o codec sem perdas para compressão, independentemente do codec selecionado por meio da política.

Para compressão com perdas: O HDX 3D Pro usa o codec original, seja o padrão ou o selecionado por meio da política.

As configurações do switch sem perdas não são retidas para sessões subsequentes. Para usar um codec sem perdas para cada conexão, selecione **Sempre sem perdas** na configuração da política de **Qualidade visual**.

- Você pode substituir o atalho padrão, ALT+SHIFT+1, para selecionar ou desmarcar Sem Perdas dentro de uma sessão. Configure uma nova configuração de registro em `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`.
  - Nome: HKLM_Hotkey, Tipo: String
  - O formato para configurar uma combinação de atalho é C=0`|`1, A=0`|`1, S=0`|`1, W=0`|`1, K=val. As chaves devem ser separadas por vírgula ",". A ordem das chaves não importa.
  - A, C, S, W e K são chaves, onde C=Control, A=ALT, S=SHIFT, W=Win, e K=uma chave válida. Os valores permitidos para K são 0–9, a–z e qualquer código de chave virtual.
  - Por exemplo:
    - Para F10, defina K=0x79
    - Para Ctrl + F10, defina C=1, K=0x79
    - Para Alt + A, defina A=1, K=a ou A=1, K=A ou K=A, A=1
    - Para Ctrl + Alt + 5, defina C=1, A=1, K=5 ou A=1, K=5, C=1
    - Para Ctrl + Shift + F5, defina A=1, S=1, K=0x74

> **Cuidado:**
>
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

- Suporte a vários monitores e monitores de alta resolução. Para máquinas de SO de sessão única, o HDX 3D Pro oferece suporte a dispositivos de usuário com até quatro monitores. Os

usuários podem organizar seus monitores em qualquer configuração e podem misturar monitores com diferentes resoluções e orientações. O número de monitores é limitado pelos recursos da GPU do computador host, do dispositivo do usuário e da largura de banda disponível. O HDX 3D Pro oferece suporte a todas as resoluções de monitor e é limitado apenas pelos recursos da GPU no computador host.

- Resolução dinâmica. Você pode redimensionar a área de trabalho virtual ou a janela do aplicativo para qualquer resolução. **Nota**: O único método suportado para alterar a resolução é redimensionando a janela da sessão VDA. A alteração da resolução de dentro da sessão VDA (usando **Painel de Controle > Aparência** e **Personalização > Vídeo > Resolução da Tela) não é suportada**.
- Suporte para arquitetura NVIDIA vGPU. O HDX 3D Pro oferece suporte a placas NVIDIA vGPU. Para obter informações, consulte NVIDIA vGPU para passthrough de GPU e compartilhamento de GPU. O NVIDIA vGPU permite que várias VMs tenham acesso simultâneo e direto a uma única GPU física, usando os mesmos drivers gráficos NVIDIA que são implantados em sistemas operacionais não virtualizados.
- Suporte para VMware vSphere e VMware ESX usando Virtual Direct Graphics Acceleration (vDGA) - Você pode usar o HDX 3D Pro com vDGA para cargas de trabalho RDS e VDI.
- Suporte para VMware vSphere/ESX usando NVIDIA vGPU e AMD MxGPU.
- Suporte para Microsoft HyperV usando Atribuição de Dispositivo Discreto no Windows Server 2016.
- Suporte para Data Center Graphics com processadores Intel Xeon E3 Family. O HDX 3D Pro oferece suporte a vários monitores (até 3), blanking de console, resolução personalizada e alta taxa de quadros com a família de processadores Intel suportada. Para obter mais informações, consulte `<http://www.citrix.com/intel>`.
- Suporte para AMD RapidFire em placas de servidor AMD FirePro série S. O HDX 3D Pro oferece suporte a vários monitores (até 6), supressão de console, resolução personalizada e alta taxa de quadros. Nota: O suporte do HDX 3D Pro para AMD MxGPU (virtualização de GPU) funciona apenas com vGPUs do VMware vSphere. XenServer e Hyper-V são suportados com passthrough de GPU. Para obter mais informações, consulte Solução de Virtualização AMD.
- Acesso a um codificador de vídeo de alto desempenho para GPUs NVIDIA, GPUs AMD e processadores gráficos Intel Iris Pro. Uma configuração de política (habilitada por padrão) controla esse recurso. O recurso permite o uso de codificação de hardware para codificação H.264 (quando disponível). Se tal hardware não estiver disponível, o VDA retorna à codificação

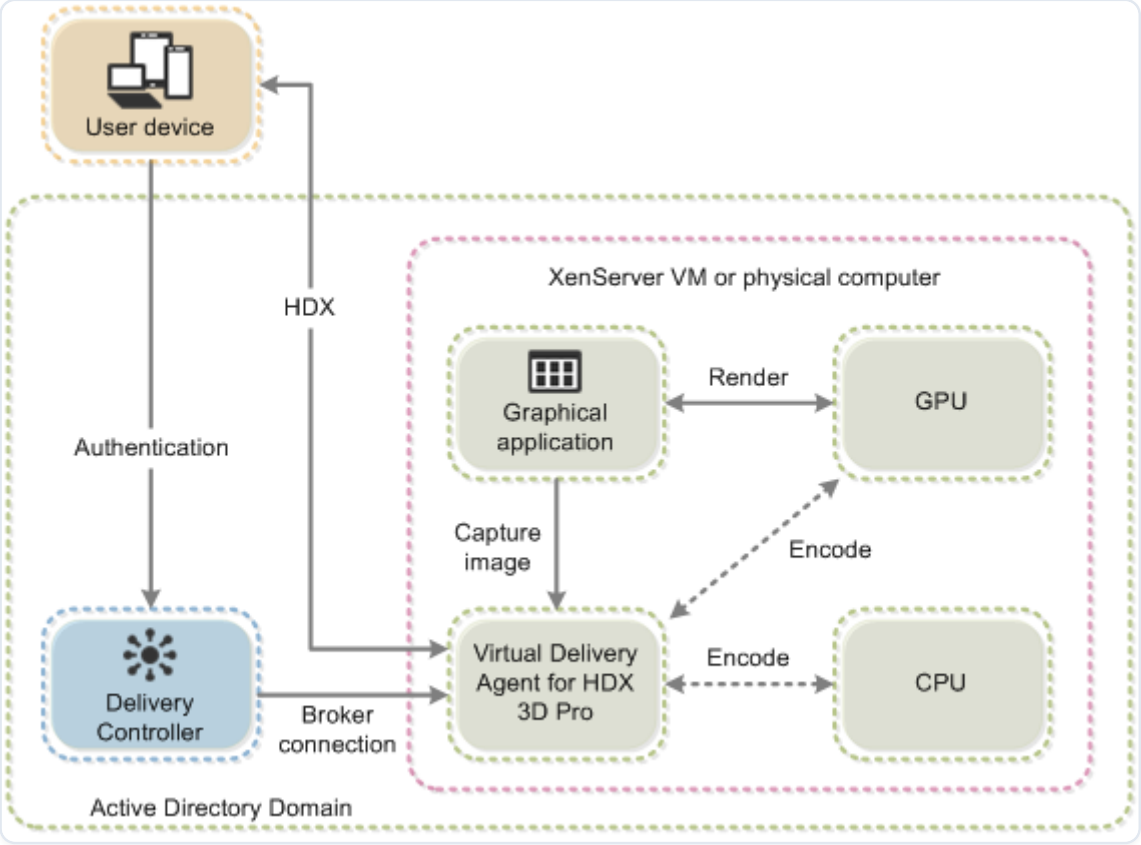
baseada em CPU usando o codec de vídeo de software. Para obter mais informações, consulte Configurações de política de gráficos.

Conforme mostrado na figura a seguir:

- Quando um usuário faz logon no aplicativo Citrix Workspace™ e acessa o aplicativo ou desktop virtual, o Controller autentica o usuário. O Controller então entra em contato com o VDA para HDX 3D Pro para intermediar uma conexão com o computador que hospeda o aplicativo gráfico.

O VDA para HDX 3D Pro usa o hardware apropriado no host para compactar as visualizações do desktop completo ou apenas do aplicativo gráfico.

- As visualizações do desktop ou aplicativo e as interações do usuário com eles são transmitidas entre o computador host e o dispositivo do usuário. Essa transmissão é feita por meio de uma conexão HDX direta entre o aplicativo Citrix Workspace e o VDA para HDX 3D Pro.



Otimizar a experiência do usuário do HDX 3D Pro

Para usar o HDX 3D Pro com vários monitores, certifique-se de que o computador host esteja configurado com pelo menos o mesmo número de monitores que estão conectados aos

dispositivos do usuário. Os monitores conectados ao computador host podem ser físicos ou virtuais.

Não conecte um monitor (físico ou virtual) a um computador host enquanto um usuário estiver conectado ao desktop ou aplicativo virtual que fornece o aplicativo gráfico. Fazer isso pode causar instabilidade durante a sessão de um usuário.

Informe seus usuários que as alterações na resolução da área de trabalho (por eles ou por um aplicativo) não são suportadas enquanto uma sessão de aplicativo gráfico está em execução. Após fechar a sessão do aplicativo, um usuário pode alterar a resolução da janela do Desktop Viewer no aplicativo Citrix Workspace - Preferências do Desktop Viewer.

Quando vários usuários compartilham uma conexão com largura de banda limitada (por exemplo, em um escritório remoto), recomendamos que você use a configuração de política **Limite geral de largura de banda da sessão** para limitar a largura de banda disponível para cada usuário. O uso dessa configuração garante que a largura de banda disponível não flutue amplamente à medida que os usuários fazem logon e logoff. Como o HDX 3D Pro se ajusta automaticamente para usar toda a largura de banda disponível, grandes variações na largura de banda disponível ao longo das sessões do usuário podem impactar negativamente o desempenho.

Por exemplo, se 20 usuários compartilharem uma conexão de 60 Mbps, a largura de banda disponível para cada usuário pode variar entre 3 Mbps e 60 Mbps, dependendo do número de usuários simultâneos. Para otimizar a experiência do usuário neste cenário, determine a largura de banda necessária por usuário nos períodos de pico e limite os usuários a essa quantidade sempre.

Para usuários de um mouse 3D, recomendamos que você aumente a prioridade do canal virtual de Redirecionamento USB Genérico para 0. Para obter informações sobre como alterar a prioridade do canal virtual, consulte o artigo da Central de Conhecimento CTX128190.

Thinwire

Introdução

Thinwire, parte da tecnologia Citrix HDX, é a tecnologia de exibição remota padrão da Citrix usada no Citrix Virtual Apps and Desktops.

A tecnologia de exibição remota permite que gráficos gerados em uma máquina sejam transmitidos, geralmente por uma rede, para outra máquina para exibição.

Uma solução de exibição remota bem-sucedida oferece uma experiência de usuário altamente interativa, semelhante à de um PC local. O Thinwire alcança essa experiência usando uma variedade de técnicas complexas e eficientes de análise e compressão de imagem. O Thinwire maximiza a escalabilidade do servidor e consome menos largura de banda do que outras tecnologias de exibição remota.

Devido a esse equilíbrio, o Thinwire atende à maioria dos casos de uso de negócios gerais e é usado como a tecnologia de exibição remota padrão no Citrix Virtual Apps and Desktops.

HDX™ 3D Pro

Em sua configuração padrão, o Thinwire pode fornecer gráficos 3D ou altamente interativos e usar uma unidade de processamento gráfico (GPU), se presente. No entanto, recomendamos habilitar o modo HDX 3D Pro usando as políticas **Otimizar para carga de trabalho de gráficos 3D** ou **Qualidade visual > Construir para sem perdas** para cenários em que GPUs estão presentes. Essas políticas configuram o Thinwire para usar um codec de vídeo (H.264 ou H.265) para codificar a tela inteira usando aceleração de hardware, se uma GPU estiver presente. Isso proporciona uma experiência mais fluida para gráficos profissionais 3D. Para obter mais informações, consulte H.264 Build to lossless, HDX 3D Pro e Aceleração de GPU para SO de sessão única do Windows.

Requisitos

O Thinwire é otimizado para sistemas operacionais modernos, incluindo Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 e Windows 10. Para Windows Server 2008 R2, o modo gráfico legado é recomendado. Use os modelos de política Citrix integrados, Alta Escalabilidade de Servidor - SO Legado e Otimizado para WAN - SO Legado para fornecer as combinações de configurações de política recomendadas pela Citrix para esses casos de uso.

> **Nota:**
>
> Não oferecemos suporte ao modo gráfico legado nesta versão. Ele está incluído para compatibilidade retroativa ao usar XenApp 7.15 LTSR, XenDesktop 7.15 LTSR e versões anteriores do VDA.

- A configuração de política que impulsiona o comportamento do Thinwire, **Usar codec de vídeo para compressão**, está disponível nas versões VDA do Citrix Virtual Apps and Desktops 7 1808 ou posterior e XenApp e XenDesktop 7.6 FP3 e posterior. A opção **Usar**

codec de vídeo quando preferencial é a configuração padrão nas versões VDA do Citrix Virtual Apps and Desktops 7 1808 ou posterior e XenApp e XenDesktop 7.9 e posterior.

- Todos os aplicativos Citrix Workspace™ suportam Thinwire. Alguns aplicativos Citrix Workspace podem suportar recursos do Thinwire que outros não, por exemplo, gráficos de 8 ou 16 bits para uso reduzido de largura de banda. O suporte para tais recursos é negociado automaticamente pelo aplicativo Citrix Workspace.
- O Thinwire usa mais recursos do servidor (CPU, memória) em cenários de vários monitores e alta resolução. É possível ajustar a quantidade de recursos que o Thinwire usa, no entanto, o uso da largura de banda pode aumentar como resultado.
- Em cenários de baixa largura de banda ou alta latência, considere habilitar gráficos de 8 ou 16 bits para melhorar a interatividade. A qualidade visual pode ser afetada, especialmente com profundidade de cor de 8 bits.

Métodos de codificação

O Thinwire pode operar em dois modos de codificação diferentes, dependendo da política e dos recursos do cliente:

- Thinwire em tela cheia H.264 ou H.265
- Thinwire com H.264 ou H.265 seletivo

O acesso remoto GDI herdado usa o driver de acesso remoto XPDM e não um codificador de bitmap Thinwire.

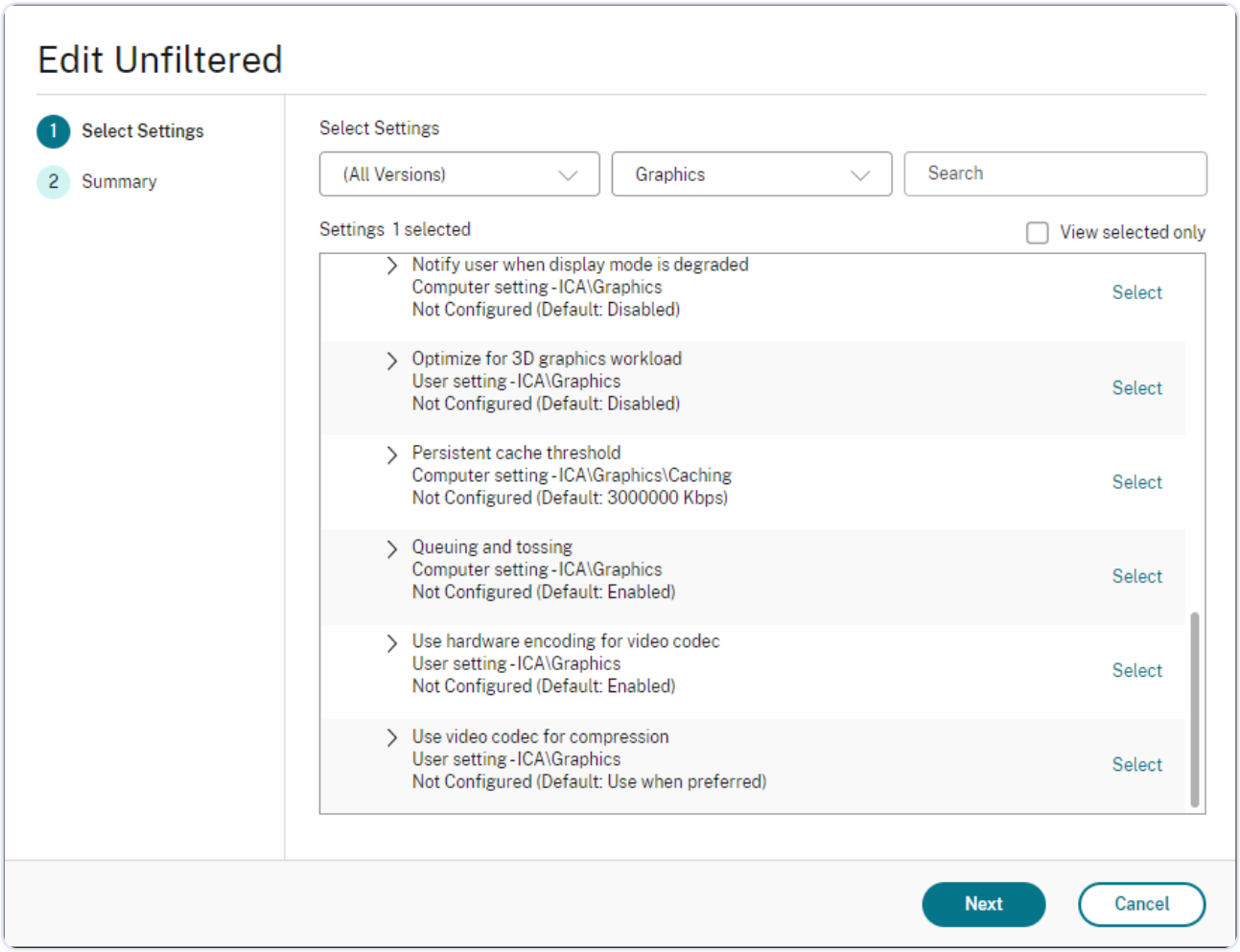
Configuração

Thinwire é a tecnologia padrão de acesso remoto de exibição.

A seguinte configuração de política de Gráficos define o padrão e oferece alternativas para diferentes casos de uso:

- Usar codec de vídeo para compactação
  - **Usar codec de vídeo quando preferível**. Esta é a configuração padrão. Nenhuma configuração adicional é necessária. Manter esta configuração como padrão garante que o Thinwire seja selecionado para todas as conexões Citrix e seja otimizado para escalabilidade, largura de banda e qualidade de imagem superior para cargas de trabalho de desktop típicas. Isso é funcionalmente equivalente a **Para regiões em mudança ativa**.

- Outras opções nesta configuração de política continuam a usar o Thinwire com outras tecnologias para diferentes casos de uso. Por exemplo:
  - **Para regiões em mudança ativa**. A tecnologia de exibição adaptativa no Thinwire identifica imagens em movimento (vídeo, 3D em movimento) e usa H.264 ou H.265 apenas na parte da tela onde a imagem está se movendo.
  - **Para a tela inteira**. Oferece Thinwire com H.264 ou H.265 em tela cheia para otimizar a experiência do usuário e a largura de banda em casos de uso intenso de gráficos 3D. No caso de H.264 4:2:0 (a política **Visualmente sem perdas** está desabilitada), a imagem final não é perfeita em pixels (sem perdas) e pode não ser adequada para certos cenários. Nesses casos, considere usar H.264 Build to lossless em vez disso.



Várias outras configurações de política, incluindo as seguintes configurações de política de exibição visual, podem ser usadas para ajustar o desempenho da tecnologia de acesso remoto de exibição. O Thinwire oferece suporte a todas elas.

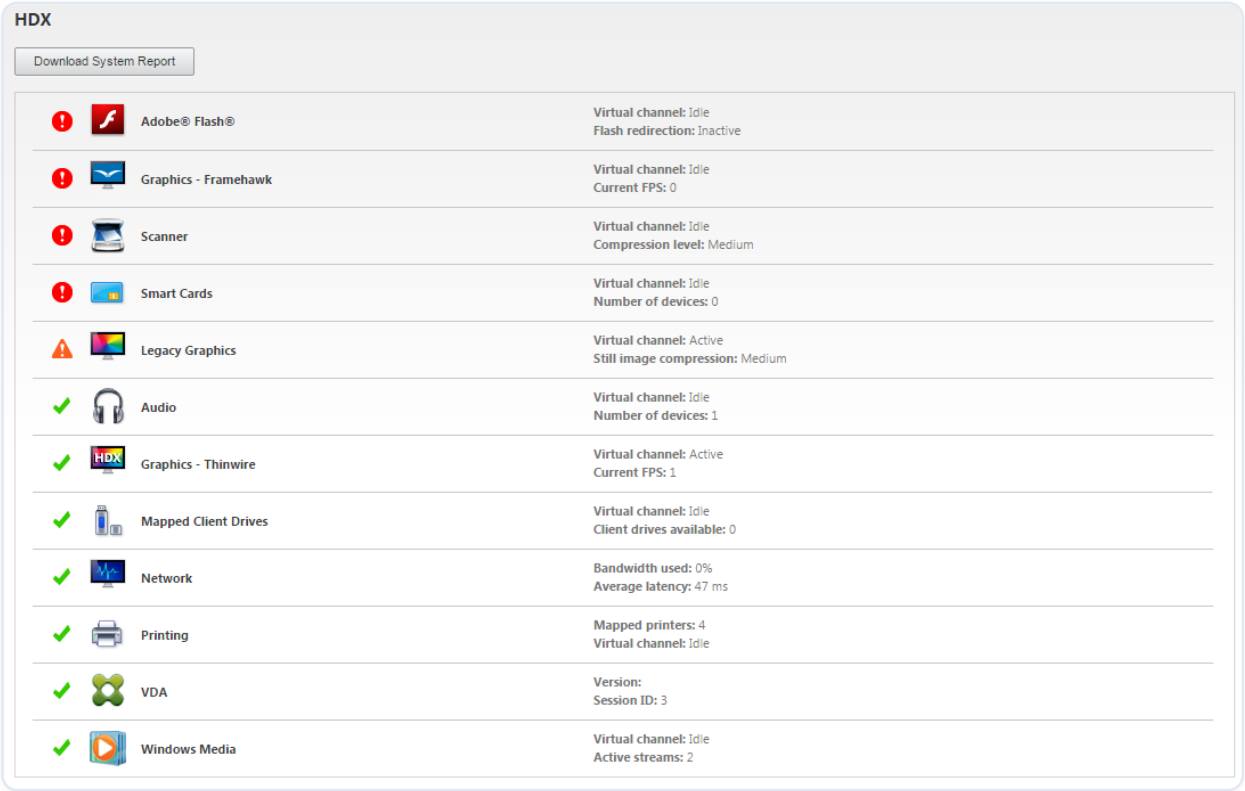
- Profundidade de cor preferida para gráficos simples
- Taxa de quadros de destino
- Qualidade visual

Para obter as combinações de configurações de política recomendadas pela Citrix para diferentes casos de uso de negócios, use os modelos de política da Citrix incorporados. Os modelos **Alta Escalabilidade de Servidor** e **Experiência de Usuário de Altíssima Definição** usam o Thinwire com as combinações ideais de configurações de política para as prioridades da sua organização e as expectativas dos seus usuários.

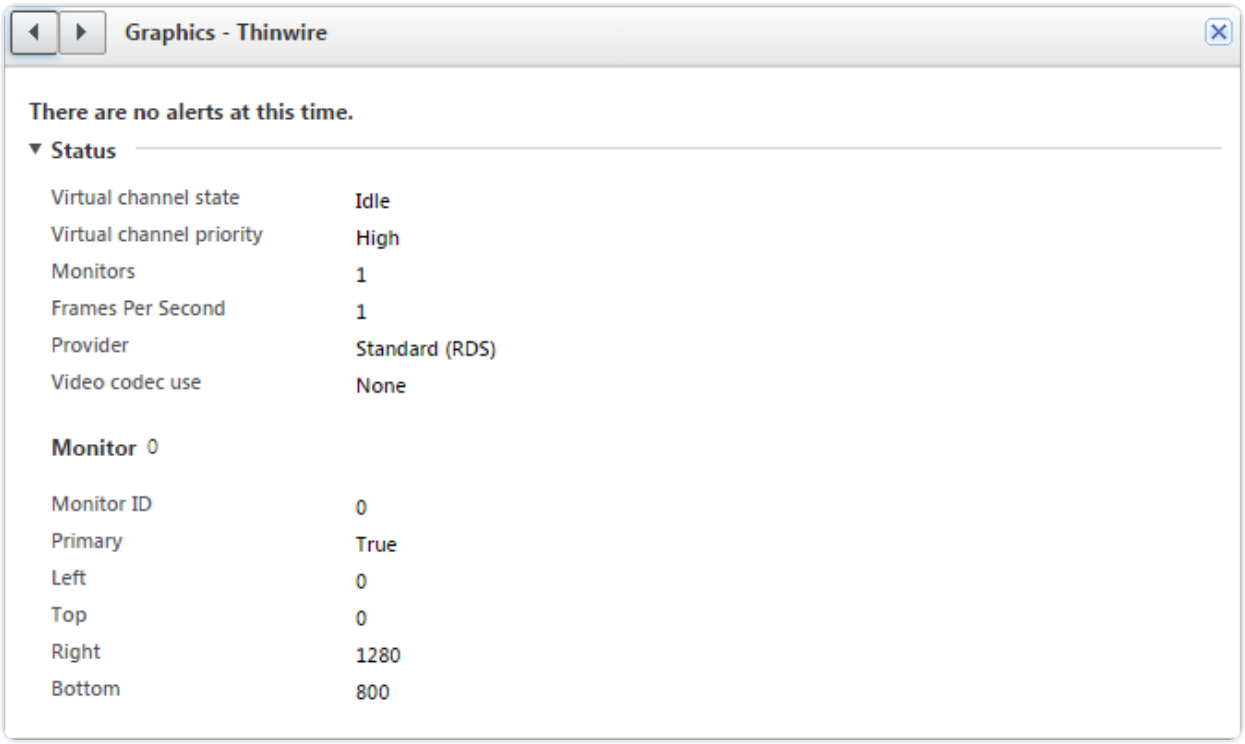
Monitorando o Thinwire

Você pode monitorar o uso e o desempenho do Thinwire no Citrix Director. A exibição de detalhes do canal virtual HDX contém informações úteis para solucionar problemas e monitorar o Thinwire em qualquer sessão. Para visualizar as métricas relacionadas ao Thinwire:

1. No Director, procure um usuário, máquina ou endpoint, abra uma sessão ativa e clique em **Detalhes**. Ou, você pode selecionar **Filtros > Sessão > Todas as Sessões**, abrir uma sessão ativa e clicar em **Detalhes**.
2. Role para baixo até o painel **HDX**.



3. Selecione **Gráficos - Thinwire**.



Codec de compressão sem perdas (MDRLE)

Em uma sessão de desktop típica, a maioria das imagens são gráficos simples ou regiões de texto. O Thinwire determina onde essas regiões estão e seleciona essas áreas para codificação sem perdas usando o codec 2DRLE. No lado do cliente do aplicativo Citrix Workspace, esses elementos são decodificados usando o decodificador 2DRLE do lado do aplicativo Citrix Workspace para exibição da sessão.

No XenApp e XenDesktop 7.17, adicionamos um codec MDRLE com taxa de compressão mais alta que consome menos largura de banda em sessões de desktop típicas do que o codec 2DRLE. Este novo codec não afeta a escalabilidade do servidor.

Menor largura de banda geralmente significa melhor interatividade da sessão (especialmente em links compartilhados ou restritos) e custos reduzidos. Por exemplo, o consumo de largura de banda esperado ao usar o codec MDRLE é aproximadamente 10–15% menor em comparação com o XenApp e XenDesktop 7.15 LTSR para cargas de trabalho típicas de escritório.

A configuração não é necessária para o codec MDRLE. Se o aplicativo Citrix Workspace suportar a decodificação MDRLE, o VDA usará a codificação MDRLE do VDA e a decodificação MDRLE do aplicativo Citrix Workspace. Se o aplicativo Citrix Workspace não suportar a decodificação MDRLE, o VDA automaticamente retornará à codificação 2DRLE.

Requisitos do MDRLE:

- Citrix Virtual Apps and Desktops versão mínima 7 1808 VDAs

- XenApp e XenDesktop versão mínima 7.17 VDAs
- Aplicativo Citrix Workspace para Windows versão mínima 1808
- Citrix Receiver para Windows versão mínima 4.11

Modo Progressivo

O Citrix Virtual Apps and Desktops 1808 introduziu o modo progressivo e o habilitou por padrão. Em condições de rede restritas (padrão: largura de banda < 2 Mbps, ou latência > 200 ms), o Thinwire aumentou a compressão de texto e imagens estáticas para melhorar a interatividade durante a atividade da tela. O texto e as imagens fortemente compactados são então progressivamente aprimorados, de forma aleatória em blocos, quando a atividade da tela é interrompida. Embora compactar e aprimorar dessa forma melhore a interatividade geral, isso reduz a eficiência do cache e aumenta o uso da largura de banda.

A partir do Citrix Virtual Apps and Desktops 1906, o modo progressivo está desabilitado por padrão. Agora usamos uma abordagem diferente. A qualidade das imagens estáticas agora é baseada nas condições da rede e flutua entre um valor mínimo e máximo predefinido para cada configuração de **Qualidade visual**. Como não há uma etapa explícita de aprimoramento, o Thinwire otimiza a entrega de imagens e mantém a eficiência do cache, ao mesmo tempo em que oferece quase todos os benefícios do modo progressivo.

Alterando o comportamento do modo progressivo

Você pode alterar o estado do modo progressivo com a chave do registro. Para obter informações, consulte Modo progressivo na lista de recursos gerenciados através do registro.

H.264 Construir para sem perdas

Construir para sem perdas é uma configuração especial do Thinwire que otimiza a entrega de gráficos para interatividade e qualidade final da imagem. Você pode habilitar essa configuração definindo a política de **Qualidade visual** como **Construir para sem perdas**.

Construir para sem perdas compacta a tela usando H.264 (ou H.265) durante a atividade da tela e aprimora para pixel perfeito (sem perdas) quando a atividade para. A qualidade da imagem H.264 (ou H.265) se adapta aos recursos disponíveis para manter a melhor taxa de quadros possível. A etapa de aprimoramento é realizada gradualmente, dando uma resposta imediata se o usuário iniciar a atividade da tela logo após o início do aprimoramento. Por exemplo, selecionar um modelo e girá-lo.

O H.264 **Build to lossless** oferece todas as vantagens do H.264 ou H.265 em tela cheia, incluindo aceleração de hardware, mas com o benefício adicional de uma tela final e garantidamente sem perdas. Isso é crítico para cargas de trabalho do tipo 3D que exigem uma imagem final perfeita em pixels. Por exemplo, manipulação de imagens médicas. Além disso, o H.264 **Build to lossless** usa menos recursos do que o H.264 4:4:4 em tela cheia. Como resultado, usar o **Build to lossless** geralmente resulta em uma taxa de quadros mais alta do que o H.264 4:4:4 visualmente sem perdas.

Nota:

Além da política de **Qualidade visual**, defina a política **Usar codec de vídeo** como **Usar quando preferencial** (padrão) ou **Para regiões em mudança ativa**. Você pode reverter para o Build to lossless não-H.264 definindo a política **Usar codec de vídeo** como **Não usar codec de vídeo**. Isso resulta em imagens em movimento sendo codificadas com JPEG em vez de H.264 (ou H.265).

Marca d'água de sessão baseada em texto

As marcas d'água de sessão baseadas em texto ajudam a impedir e permitir o rastreamento de roubo de dados. Essas informações rastreáveis aparecem na área de trabalho da sessão como um impedimento para aqueles que usam fotografias e capturas de tela para roubar dados. Você pode especificar uma marca d'água que é uma camada de texto, que é exibida em toda a tela da sessão sem alterar o conteúdo do documento original. As marcas d'água de sessão baseadas em texto exigem suporte VDA.

Importante:

A marca d'água de sessão baseada em texto não é um recurso de segurança. A solução não impede completamente o roubo de dados, mas oferece algum nível de impedimento e rastreabilidade. Embora não garantamos a rastreabilidade completa das informações ao usar esse recurso, recomendamos que você o combine com outras soluções de segurança, conforme aplicável.

A marca d'água da sessão é um texto e é aplicada à sessão que é entregue ao usuário. A marca d'água da sessão contém informações para rastrear o roubo de dados. Os dados mais importantes são a identidade do usuário de logon da sessão atual na qual a imagem da

> tela foi tirada. Para rastrear o vazamento de dados com mais eficácia, inclua outras informações, como o endereço IP do servidor ou cliente e um tempo de conexão.

Para ajustar a experiência do usuário, use as configurações de política de marca d'água da sessão para configurar o posicionamento e a aparência da marca d'água na tela.

Requisitos:

Virtual Delivery Agents:

SO multissessão 7.17 SO de sessão única 7.17

Limitações:

- As marcas d'água de sessão não são suportadas em sessões onde são usados Local App Access, redirecionamento de mídia do Windows, MediaStream, redirecionamento de conteúdo do navegador e redirecionamento de vídeo HTML5. Para usar a marca d'água de sessão, certifique-se de que esses recursos estejam desativados.
- A marca d'água de sessão não é suportada e não aparece se a sessão estiver sendo executada em modos acelerados por hardware em tela cheia (codificação H.264 ou H.265 em tela cheia).
- Se você definir estas políticas HDX™, as configurações de marca d'água não terão efeito e uma marca d'água não será exibida na sessão.

Usar codificação de hardware para codec de vídeo para **Ativado Usar codec de vídeo para compactação** para **Para a tela inteira**

- Se você definir essas políticas HDX, o comportamento será indeterminado e a marca d'água poderá não ser exibida.

  Usar codificação de hardware para codec de vídeo para **Ativado Usar codec de vídeo para compactação** para **Usar codec de vídeo quando preferido**

  Para garantir que a marca d'água seja exibida, defina **Usar codificação de hardware para codec de vídeo** como **Desativado**, ou defina **Usar codec de vídeo para compactação** como **Para regiões em mudança ativa** ou **Não usar codec de vídeo**.
- A marca d'água de sessão suporta apenas o modo gráfico Thinwire.
- Se você usar a Gravação de Sessão, a sessão gravada não incluirá a marca d'água.
- Se você usar a assistência remota do Windows, a marca d'água não será exibida.

- Se um usuário pressionar a tecla **Print Screen** para capturar a tela, a tela capturada no lado do VDA não incluirá as marcas d'água. Recomendamos que você tome medidas para evitar que a imagem capturada seja copiada.

Multimídia

A pilha de tecnologia HDX™ oferece suporte à entrega de aplicativos multimídia por meio de duas abordagens complementares:

- Entrega de multimídia com renderização no lado do servidor
- Redirecionamento de multimídia com renderização no lado do cliente

Essa estratégia garante que você possa entregar uma gama completa de formatos multimídia, com uma ótima experiência do usuário, enquanto maximiza a escalabilidade do servidor para reduzir o custo por usuário.

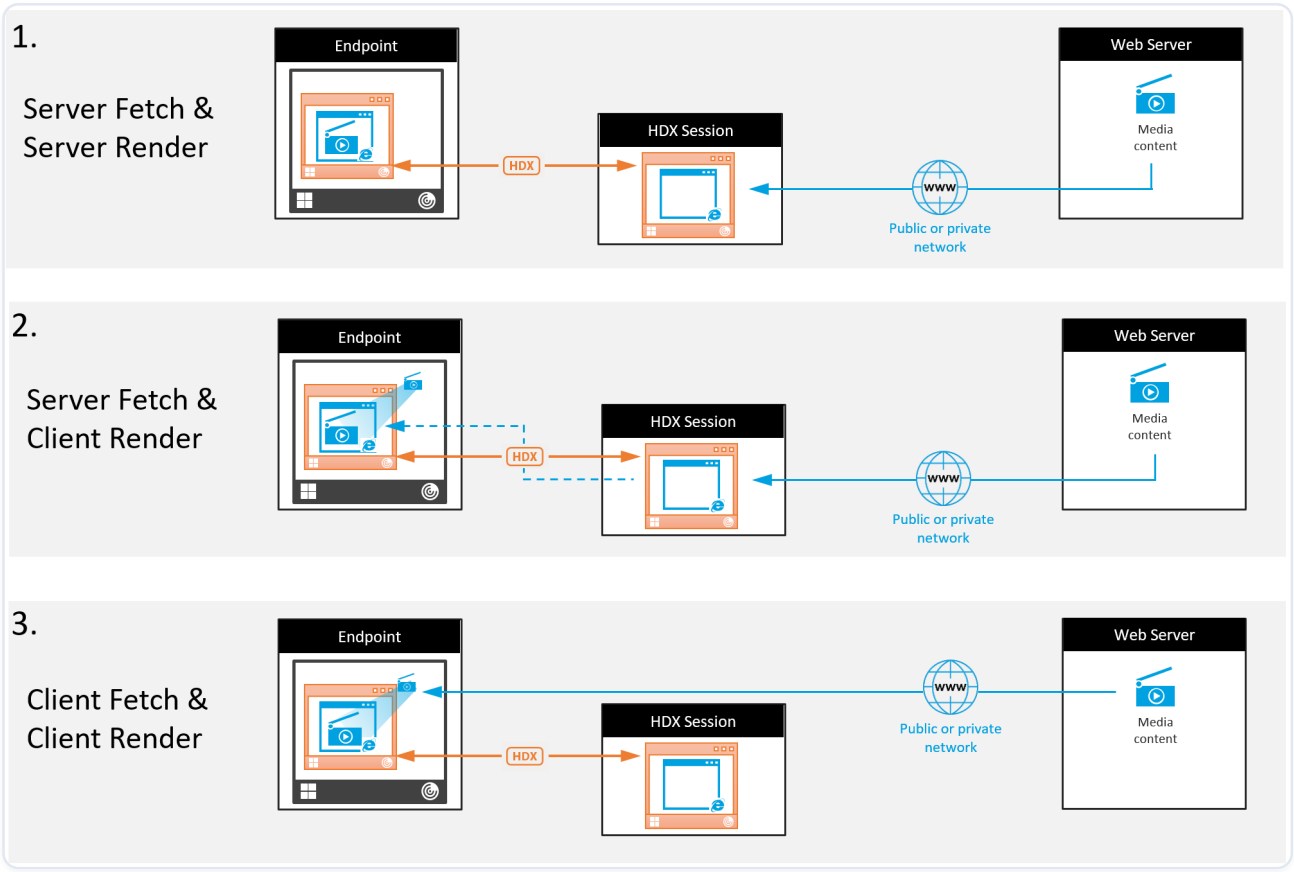
Com a entrega de multimídia renderizada no servidor, o conteúdo de áudio e vídeo é decodificado e renderizado no servidor Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) pelo aplicativo. O conteúdo é então compactado e entregue usando o protocolo ICA para o aplicativo Citrix Workspace no dispositivo do usuário. Esse método oferece a maior taxa de compatibilidade com vários aplicativos e formatos de mídia. Como o processamento de vídeo exige muito processamento, a entrega de multimídia renderizada no servidor se beneficia muito da aceleração de hardware integrada. Por exemplo, o suporte para DirectX Video Acceleration (DXVA) descarrega a CPU realizando a decodificação H.264 em hardware separado. As tecnologias Intel Quick Sync, AMD RapidFire e NVIDIA NVENC fornecem codificação H.264 acelerada por hardware.

Como a maioria dos servidores não oferece nenhuma aceleração de hardware para compactação de vídeo, a escalabilidade do servidor é impactada negativamente se todo o processamento de vídeo for feito na CPU do servidor. Você pode manter alta escalabilidade do servidor, redirecionando muitos formatos multimídia para o dispositivo do usuário para renderização local.

- O redirecionamento do Windows Media descarrega o servidor para uma ampla variedade de formatos de mídia tipicamente associados ao Windows Media Player.
- O vídeo HTML5 tornou-se popular, e a Citrix® introduziu uma tecnologia de redirecionamento para esse tipo de conteúdo. Recomendamos o redirecionamento de conteúdo do navegador para sites que usam HTML5, HLS, DASH ou WebRTC.
- Você pode aplicar as tecnologias gerais de redirecionamento de contato Redirecionamento Host-para-cliente e Acesso a Aplicativos Locais ao conteúdo multimídia.

Juntando essas tecnologias, se você não configurar o redirecionamento, o HDX fará a Renderização no Lado do Servidor. Se você configurar o redirecionamento, o HDX usará a Busca no Servidor e Renderização no Cliente ou a Busca no Cliente e Renderização no Cliente. Se esses métodos falharem, o HDX retornará à Renderização no Lado do Servidor conforme necessário e estará sujeito à Política de Prevenção de Fallback.

Cenários de exemplo



Cenário 1. (Busca no Servidor e Renderização no Servidor):

1. O servidor busca o arquivo de mídia de sua origem, decodifica e, em seguida, apresenta o conteúdo a um dispositivo de áudio ou dispositivo de exibição.
2. O servidor extrai a imagem ou o som apresentados do dispositivo de exibição ou do dispositivo de áudio, respectivamente.
3. O servidor, opcionalmente, o compacta e, em seguida, o transmite para o cliente.

Essa abordagem incorre em alto custo de CPU, alto custo de largura de banda (se a imagem/som extraído não for compactado de forma eficiente) e tem baixa escalabilidade do servidor.

Os canais virtuais Thinwire e Áudio manipular essa abordagem. A vantagem dessa abordagem é que ela reduz os requisitos de hardware e software para os clientes. Usando essa abordagem, a

decodificação acontece no servidor e funciona para uma variedade maior de dispositivos e formatos.

Cenário 2. (Busca pelo Servidor e Renderização pelo Cliente):

Essa abordagem depende da capacidade de interceptar o conteúdo de mídia antes que ele seja decodificado e apresentado ao dispositivo de áudio ou exibição. O conteúdo de áudio/vídeo compactado é enviado ao cliente, onde é então decodificado e apresentado localmente. A vantagem dessa abordagem é que as tarefas são descarregadas para os dispositivos cliente, economizando ciclos de CPU no servidor.

No entanto, ela também introduz alguns requisitos adicionais de hardware e software para o cliente. O cliente deve ser capaz de decodificar cada formato que possa receber.

Cenário 3. (Busca pelo Cliente e Renderização pelo Cliente):

Essa abordagem depende da capacidade de interceptar a URL do conteúdo de mídia antes que ela seja buscada da origem. A URL é enviada ao cliente, onde o conteúdo de mídia é buscado, decodificado e apresentado localmente. Essa abordagem é conceitualmente simples. Sua vantagem é que ela economiza ciclos de CPU no servidor e largura de banda, pois o servidor envia apenas comandos de controle. No entanto, o conteúdo de mídia nem sempre está acessível aos clientes.

Estrutura e plataforma:

Sistemas operacionais de sessão única (Windows, Mac OS X e Linux) fornecem estruturas multimídia que permitem o desenvolvimento mais rápido de aplicativos multimídia. Esta tabela lista algumas das estruturas multimídia mais populares. Cada estrutura divide o processamento de mídia em várias etapas e usa uma arquitetura baseada em pipeline.

ESTRUTURA	PLATAFORMA
DirectShow	Windows (98 e posterior)
Media Foundation	Windows (Vista e posterior)
Gstreamer	Linux
Quicktime	Mac OS X

Suporte a salto duplo com tecnologias de redirecionamento de mídia

Redirecionamento de áudio	Não
Redirecionamento de conteúdo do navegador	Não
Redirecionamento de webcam HDX	Sim
Redirecionamento de vídeo HTML5	Sim
Redirecionamento de Mídia do Windows	Sim

Áudio

Você pode configurar e adicionar as seguintes configurações de política do Citrix a uma política que otimiza os recursos de áudio HDX. Para detalhes de uso, além de relacionamentos e dependências com outras configurações de política, consulte Configurações de política de áudio, Configurações de política de largura de banda e Configurações de política de conexões multi-stream.

> **Importante:**
>
> Recomendamos a entrega de áudio usando o User Datagram Protocol (UDP) em vez de TCP. Somente o Windows Virtual Delivery Agent (VDA) oferece suporte a áudio sobre UDP.
>
> A criptografia de áudio UDP usando DTLS está disponível apenas entre o Citrix Gateway e o aplicativo Citrix Workspace™. Portanto, às vezes pode ser preferível usar o transporte TCP. O TCP oferece suporte à criptografia TLS de ponta a ponta do VDA para o aplicativo Citrix Workspace.

Qualidade do áudio

Em geral, uma qualidade de som mais alta consome mais largura de banda e utilização da CPU do servidor, enviando mais dados de áudio para os dispositivos do usuário. A compressão de som permite equilibrar a qualidade do som com o desempenho geral da sessão; use as configurações

de política do Citrix para configurar os níveis de compressão a serem aplicados aos arquivos de som.

Por padrão, a configuração da **política de qualidade de áudio** é definida como Alta - áudio de alta definição quando o transporte TCP é usado. A política é definida como Média - otimizada para fala quando o transporte UDP (recomendado) é usado. A configuração de **áudio de alta definição** fornece áudio estéreo de alta fidelidade, mas consome mais largura de banda do que outras configurações de qualidade. Não use esta qualidade de áudio para aplicativos de chat de voz ou vídeo não otimizados (como softphones). A razão é que isso pode introduzir latência no caminho do áudio que não é adequada para comunicações em tempo real. Recomendamos a configuração de política otimizada para fala para áudio em tempo real, independentemente do protocolo de transporte selecionado.

Quando a largura de banda é limitada, por exemplo, conexões via satélite ou discadas, reduzir a qualidade do áudio para **Baixa** consome a menor largura de banda possível. Nesta situação, crie políticas separadas para usuários em conexões de baixa largura de banda para que os usuários em conexões de alta largura de banda não sejam afetados negativamente.

Para detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Diretrizes de largura de banda para reprodução e gravação de áudio:

- Alta qualidade (padrão)
  - Taxa de bits: ~100 kbps (mín. 75, máx. 175 kbps) para reprodução / ~70 kbps para captura de microfone
  - Número de Canais: 2 (Estéreo) para reprodução, 1 (mono) para captura de microfone
  - Frequência: 44100 Hz
  - Profundidade de bits: 16 bits
- Qualidade média (recomendado para VoIP)
  - Taxa de bits: ~16 kbps (mín. 20, máx. 40 kbps) para reprodução, ~16 kbps para captura de microfone
  - Número de Canais: 1 (Mono) para reprodução e captura
  - Frequência: 16000 Hz (banda larga)
  - Profundidade de bits: 16 bits
- Qualidade baixa

- Taxa de bits: ~ 11 kbps (mín. 10; máx. 25 kbps) para reprodução, ~11 kbps para captura de microfone
- Número de Canais: 1 (Mono) para reprodução e captura
- Frequência: 8000 Hz (banda estreita)
- Profundidade de bits: 16 bits

Redirecionamento de áudio do cliente

Para permitir que os usuários recebam áudio de um aplicativo em um servidor através de alto-falantes ou outros dispositivos de som no dispositivo do usuário, deixe a configuração de **Redirecionamento de áudio do cliente** como **Permitido**. Esta é a configuração padrão.

O mapeamento de áudio do cliente coloca uma carga extra nos servidores e na rede. No entanto, proibir o redirecionamento de áudio do cliente desativa toda a funcionalidade de áudio HDX™.

Para obter detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Redirecionamento de microfone do cliente

Para permitir que os usuários gravem áudio usando dispositivos de entrada, como microfones no dispositivo do usuário, deixe a configuração **Redirecionamento de microfone do cliente** em seu padrão (Permitido).

Por segurança, os dispositivos do usuário alertam seus usuários quando servidores em que não confiam tentam acessar microfones. Os usuários podem optar por aceitar ou rejeitar o acesso antes de usar o microfone. Os usuários podem desativar este alerta no aplicativo Citrix Workspace.

Para obter detalhes da configuração, consulte Configurações de política de áudio. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Plug N Play de áudio

A configuração de política Plug N Play de áudio permite ou impede o uso de vários dispositivos de áudio para gravar e reproduzir som. Essa configuração está **Habilitada** por padrão. O Plug N Play de áudio permite que os dispositivos de áudio sejam reconhecidos. Os dispositivos são reconhecidos mesmo que não estejam conectados até depois do início da sessão do usuário.

Essa configuração se aplica apenas a máquinas com sistema operacional Windows multissessão.

Para obter detalhes da configuração, consulte Configurações de política de áudio.

Limite de largura de banda de redirecionamento de áudio e porcentagem de limite de largura de banda de redirecionamento de áudio

A configuração de política Limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima (em kilobits por segundo) para reprodução e gravação de áudio em uma sessão.

A configuração Porcentagem de limite de largura de banda de redirecionamento de áudio especifica a largura de banda máxima para redirecionamento de áudio como uma porcentagem da largura de banda total disponível.

Por padrão, zero (sem máximo) é especificado para ambas as configurações. Se ambas as configurações forem configuradas, a que tiver o menor limite de largura de banda será usada.

Para obter detalhes da configuração, consulte Configurações de política de largura de banda. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Áudio sobre transporte em tempo real UDP e intervalo de porta UDP de áudio

Por padrão, o Áudio sobre Transporte em Tempo Real do Protocolo de Datagrama de Usuário (UDP) é permitido (quando selecionado no momento da instalação). Ele abre uma porta UDP no servidor para conexões que usam Áudio sobre Transporte em Tempo Real UDP. Se houver congestionamento de rede ou perda de pacotes, recomendamos configurar UDP/RTP para áudio para garantir a melhor experiência possível ao usuário. Para qualquer áudio em tempo real, como aplicativos de softphone, o áudio UDP é preferível ao EDT. O UDP permite a perda de pacotes sem retransmissão, garantindo que nenhuma latência seja adicionada em conexões com alta perda de pacotes.

> **Importante:**
>
> Quando o Citrix Gateway não está no caminho, os dados de áudio transmitidos com UDP não são criptografados. Se o Citrix Gateway estiver configurado para acessar recursos do Citrix Virtual Apps and Desktops™, o tráfego de áudio entre o dispositivo de endpoint e o Citrix Gateway é protegido usando o protocolo DTLS.

> O intervalo de portas UDP de áudio especifica o intervalo de números de porta que o VDA do Windows usa para trocar dados de pacotes de áudio com o dispositivo do usuário.

Por padrão, o intervalo é de 16500 a 16509.

Para obter detalhes de configuração sobre Áudio sobre UDP Real-time Transport, consulte Configurações de política de áudio. Para obter detalhes sobre o intervalo de portas UDP de áudio, consulte Configurações de política de conexões multi-stream. Lembre-se de habilitar as configurações de áudio do cliente no dispositivo do usuário.

Áudio sobre UDP requer o VDA do Windows. Para políticas suportadas no VDA do Linux, consulte Lista de suporte de políticas.

Políticas de configuração de áudio para dispositivos de usuário

1. Carregue os modelos de política de grupo seguindo Configurando o modelo administrativo do Objeto de Política de Grupo.
2. No Editor de Política de Grupo, expanda **Modelos Administrativos > Componentes Citrix > Citrix Workspace > Experiência do Usuário**.
3. Para **Configurações de áudio do cliente**, selecione **Não Configurado**, **Habilitado** ou **Desabilitado**.
    - **Não Configurado**. Por padrão, o Redirecionamento de Áudio é habilitado usando áudio de alta qualidade ou as configurações de áudio personalizadas configuradas anteriormente.
    - **Habilitado**. Habilita o redirecionamento de áudio usando as opções selecionadas.
    - **Desabilitado**. Desabilita o redirecionamento de áudio.
4. Se você selecionar **Habilitado**, escolha uma qualidade de som. Para áudio UDP, use **Médio** (padrão).
5. Apenas para áudio UDP, selecione **Habilitar Transporte em Tempo Real** e então defina o intervalo de portas de entrada a serem abertas no firewall local do Windows.
6. Para usar Áudio UDP com Citrix Gateway, selecione **Permitir Transporte em Tempo Real Através do gateway**. Configure o Citrix Gateway com DTLS. Para mais informações, consulte este artigo.

Como Administrador, se você não tiver controle sobre os dispositivos de endpoint para fazer essas alterações, use os atributos default.ica do StoreFront para habilitar o Áudio UDP. Por exemplo, para dispositivos pessoais ou computadores domésticos.

1. Na máquina StoreFront, abra C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica com um editor como o notepad.
2. Faça as seguintes entradas na seção .

   ; Este texto habilita o Transporte em Tempo Real

   EnableRtpAudio=true

   ; Este texto permite o Transporte em Tempo Real Através do gateway

   EnableUDPThroughGateway=true

   ; Este texto define a qualidade do áudio como Média

   AudioBandwidthLimit=1

   ; Intervalo de portas UDP

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

Se você habilitar o áudio do User Datagram Protocol (UDP) editando default.ica, o áudio UDP será habilitado para todos os usuários que estiverem usando essa loja.

Evitar eco durante conferências multimídia

Usuários em conferências de áudio ou vídeo podem ouvir um eco. Ecos geralmente ocorrem quando alto-falantes e microfones estão muito próximos um do outro. Por esse motivo, recomendamos o uso de fones de ouvido para conferências de áudio e vídeo.

O HDX oferece uma opção de cancelamento de eco (habilitada por padrão) que minimiza qualquer eco. A eficácia do cancelamento de eco é sensível à distância entre os alto-falantes e o microfone. Certifique-se de que os dispositivos não estejam muito próximos ou muito distantes um do outro.

Você pode alterar uma configuração de registro para desabilitar o cancelamento de eco. Para obter informações, consulte Evitar eco durante conferências multimídia na lista de recursos gerenciados por meio do registro.

Softphones

Um softphone é um software que atua como uma interface de telefone. Você usa um softphone para fazer chamadas pela internet a partir de um computador ou outro dispositivo inteligente. Ao usar um softphone, você pode discar números de telefone e realizar outras funções relacionadas ao telefone usando uma tela.

O Citrix Virtual Apps and Desktops oferece suporte a várias alternativas para a entrega de softphones.

- **Modo de controle**. O softphone hospedado controla um aparelho telefônico físico. Neste modo, nenhum tráfego de áudio passa pelo servidor Citrix Virtual Apps and Desktops.
- **Suporte a softphone otimizado para HDX RealTime (recomendado)**. O mecanismo de mídia é executado no dispositivo do usuário, e o tráfego de Voz sobre Protocolo de Internet flui de ponto a ponto. Para exemplos, consulte:
  - Otimização HDX para Microsoft Teams
  - HDX RealTime Optimization Pack, que otimiza a entrega do Microsoft Skype for Business
  - Cisco Jabber Softphone para VDI (anteriormente conhecido como VXME)
  - Cisco Webex Meetings para VDI
  - Avaya VDI Equinox (anteriormente conhecido como VDI Communicator)
  - Plugin VDI do Zoom
  - Genesys PureEngage Cloud
  - Dispositivo de ditado Nuance Dragon PowerMic
- **Acesso a Aplicativos Locais**. Um recurso do Citrix Virtual Apps and Desktops e Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) que permite que um aplicativo, como um softphone, seja executado localmente no dispositivo Windows do usuário, mas apareça perfeitamente integrado ao seu desktop virtual/publicado. Esse recurso descarrega todo o processamento de áudio para o dispositivo do usuário. Para obter mais informações, consulte Acesso a Aplicativos Locais e redirecionamento de URL.
- **Suporte genérico a softphone HDX RealTime.** Voz sobre Protocolo de Internet sobre ICA.

Suporte genérico a softphone

O suporte genérico a softphone permite hospedar um softphone não modificado no XenApp ou XenDesktop no datacenter. O tráfego de áudio passa pelo protocolo Citrix ICA (preferencialmente usando UDP/RTP) para o dispositivo do usuário que executa o aplicativo Citrix Workspace.

O suporte genérico a softphone é um recurso do HDX RealTime. Essa abordagem para entrega de softphone é especialmente útil quando:

- Uma solução otimizada para entregar o softphone não está disponível e o usuário não está em um dispositivo Windows onde o Acesso a Aplicativos Locais possa ser usado.
- O mecanismo de mídia necessário para a entrega otimizada do softphone não está instalado no dispositivo do usuário ou não está disponível para a versão do sistema operacional em execução no dispositivo do usuário. Nesse cenário, o HDX RealTime Genérico fornece uma solução de fallback valiosa.

Existem duas considerações sobre a entrega de softphone usando Citrix Virtual Apps and Desktops:

- Como o aplicativo softphone é entregue ao desktop virtual/publicado.
- Como o áudio é entregue para e do headset, microfone e alto-falantes do usuário, ou conjunto de telefone USB.

Citrix Virtual Apps and Desktops incluem inúmeras tecnologias para suportar a entrega genérica de softphone:

- Codec otimizado para fala para codificação rápida do áudio em tempo real e eficiência de largura de banda.
- Pilha de áudio de baixa latência.
- Buffer de jitter do lado do servidor para suavizar o áudio quando a latência da rede flutua.
- Marcação de pacotes (DSCP e WMM) para Qualidade de Serviço.
    - Marcação DSCP para pacotes RTP (Camada 3)
    - Marcação WMM para Wi-Fi

As versões do aplicativo Citrix Workspace para Windows, Linux, Chrome e Mac também são compatíveis com Voz sobre Protocolo de Internet. O aplicativo Citrix Workspace para Windows oferece estes recursos:

- Buffer de jitter do lado do cliente - Garante áudio suave mesmo quando a latência da rede flutua.
- Cancelamento de eco - Permite maior variação na distância entre o microfone e os alto-falantes para trabalhadores que não usam fone de ouvido.
- Áudio plug-n-play - Dispositivos de áudio não precisam ser conectados antes de iniciar uma sessão. Eles podem ser conectados a qualquer momento.

- Roteamento de dispositivo de áudio - Os usuários podem direcionar o toque para os alto-falantes, mas o caminho de voz para o fone de ouvido.
- ICA multi-stream - Permite roteamento flexível baseado em Qualidade de Serviço pela rede.
- O ICA suporta quatro fluxos TCP e dois UDP. Um dos fluxos UDP suporta o áudio em tempo real sobre RTP.

Para um resumo dos recursos do aplicativo Citrix Workspace, consulte Matriz de Recursos do Citrix Receiver.

Recomendações de configuração do sistema

Hardware e Software do Cliente: Para uma qualidade de áudio ideal, recomendamos a versão mais recente do aplicativo Citrix Workspace e um fone de ouvido de boa qualidade que tenha cancelamento de eco acústico (AEC). As versões do aplicativo Citrix Workspace para Windows, Linux e Mac suportam Voz sobre Protocolo de Internet. Além disso, a Dell Wyse oferece suporte a Voz sobre Protocolo de Internet para ThinOS (WTOS).

Considerações sobre a CPU: Monitore o uso da CPU no VDA para determinar se é necessário atribuir duas CPUs virtuais a cada máquina virtual. Voz e vídeo em tempo real são intensivos em dados. A configuração de duas CPUs virtuais reduz a latência de troca de threads. Portanto, recomendamos que você configure duas vCPUs em um ambiente VDI do Citrix Virtual Desktops™.

Ter duas CPUs virtuais não significa necessariamente dobrar o número de CPUs físicas, pois as CPUs físicas podem ser compartilhadas entre sessões.

O Citrix Gateway Protocol (CGP), que é usado para o recurso de Confiabilidade da Sessão, também aumenta o consumo de CPU. Em conexões de rede de alta qualidade, você pode desabilitar esse recurso para reduzir o consumo de CPU no VDA. Nenhuma das etapas anteriores pode ser necessária em um servidor poderoso.

Áudio UDP: O áudio sobre UDP oferece excelente tolerância a congestionamento de rede e perda de pacotes. Recomendamos usá-lo em vez de TCP quando disponível.

Configuração de LAN/WAN: A configuração adequada da rede é fundamental para uma boa qualidade de áudio em tempo real. Normalmente, você deve configurar redes locais virtuais (VLANs) porque pacotes de broadcast excessivos podem introduzir jitter. Dispositivos habilitados para IPv6 podem gerar muitos pacotes de broadcast. Se o suporte a IPv6 não for necessário, você pode desabilitar o IPv6 nesses dispositivos. Configure para suportar Qualidade de Serviço.

Configurações para uso de conexões WAN: Você pode usar bate-papo por voz em conexões LAN e WAN. Em uma conexão WAN, a qualidade do áudio depende da latência, perda de pacotes e jitter na conexão. Se estiver entregando softphones para usuários em uma conexão WAN, recomendamos usar o NetScaler® SD-WAN entre o data center e o escritório remoto. Isso mantém uma alta Qualidade de Serviço. O NetScaler SD-WAN suporta ICA Multi-Stream, incluindo UDP. Além disso, para um único fluxo TCP, é possível distinguir as prioridades de vários canais virtuais ICA para garantir que os dados de áudio em tempo real de alta prioridade recebam tratamento preferencial.

Use o Director ou o HDX Monitor para validar sua configuração HDX.

Conexões de usuário remoto: O Citrix Gateway suporta DTLS para entregar tráfego UDP/RTP nativamente (sem encapsulamento em TCP). Abra os firewalls bidirecionalmente para tráfego UDP na Porta 443.

Seleção de codec e consumo de largura de banda: Entre o dispositivo do usuário e o VDA no data center, recomendamos usar a configuração de codec **Otimizado para Fala**, também conhecida como áudio de Qualidade Média. Entre a plataforma VDA e o IP-PBX, o softphone usa o codec configurado ou negociado. Por exemplo:

- G711 oferece boa qualidade de voz, mas tem um requisito de largura de banda de 80 kilobits por segundo a 100 kilobits por segundo por chamada (dependendo das sobrecargas da Camada 2 da Rede).
- G729 oferece boa qualidade de voz e tem um baixo requisito de largura de banda de 30 kilobits por segundo a 40 kilobits por segundo por chamada (dependendo das sobrecargas da Camada 2 da Rede).

Entrega de aplicativos de softphone para o desktop virtual

Existem dois métodos pelos quais você pode entregar um softphone para o desktop virtual XenDesktop®:

- O aplicativo pode ser instalado na imagem do desktop virtual.
- O aplicativo pode ser transmitido por streaming para o desktop virtual usando o Microsoft App-V. Essa abordagem tem vantagens de gerenciamento porque a imagem do desktop virtual é mantida organizada. Após ser transmitido por streaming para o desktop virtual, o aplicativo é executado nesse ambiente como se tivesse sido instalado da maneira usual. Nem todos os aplicativos são compatíveis com o App-V.

Entrega de áudio para e do dispositivo do usuário

O HDX RealTime genérico suporta dois métodos de entrega de áudio para e do dispositivo do usuário:

- **Canal Virtual de Áudio Citrix**. Geralmente recomendamos o Canal Virtual de Áudio Citrix porque ele foi projetado especificamente para transporte de áudio.
- **Redirecionamento USB Genérico**. Suporta dispositivos de áudio com botões ou um display (ou ambos), dispositivo de interface humana (HID), se o dispositivo do usuário estiver em uma conexão LAN ou similar à LAN de volta para o servidor Citrix Virtual Apps and Desktops.

Canal virtual de áudio Citrix

O Canal Virtual de Áudio Citrix bidirecional (CTXCAM) permite que o áudio seja entregue eficientemente pela rede. O HDX RealTime Genérico pega o áudio do headset ou microfone do usuário e o compacta. Em seguida, ele o envia via ICA para o aplicativo de softphone no desktop virtual. Da mesma forma, a saída de áudio do softphone é compactada e enviada na outra direção para o headset ou alto-falantes do usuário. Essa compactação é independente da compactação usada pelo próprio softphone (como G.729 ou G.711). Ela é feita usando o codec Otimizado para Fala (Qualidade Média). Suas características são ideais para Voz sobre Protocolo de Internet. Ele apresenta tempo de codificação rápido e consome apenas aproximadamente 56 Kilobits por segundo de largura de banda da rede (28 Kbps em cada direção), no pico. Este codec deve ser explicitamente selecionado no console de Gerenciamento do serviço porque não é o codec de áudio padrão. O padrão é o codec de Áudio HD (Alta Qualidade). Este codec é excelente para trilhas sonoras estéreo de alta fidelidade, mas é mais lento para codificar em comparação com o codec Otimizado para Fala.

Redirecionamento USB Genérico

A tecnologia de Redirecionamento USB Genérico da Citrix (canal virtual CTXGUSB) fornece um meio genérico de acesso remoto a dispositivos USB, incluindo dispositivos compostos (áudio mais HID) e dispositivos USB isócronos. Essa abordagem é limitada a usuários conectados à LAN. A razão é que o protocolo USB tende a ser sensível à latência da rede e requer uma largura de banda considerável. O redirecionamento USB isócrono funciona bem ao usar alguns softphones. Este redirecionamento oferece excelente qualidade de voz e baixa latência. No entanto, o Canal Virtual de Áudio Citrix é preferido porque é otimizado para tráfego de áudio. A principal exceção é quando você está usando um dispositivo de áudio com botões. Por exemplo, um telefone USB conectado ao dispositivo do usuário que está conectado à LAN do data center. Neste caso, o Redirecionamento USB Genérico suporta botões no aparelho telefônico ou headset que controlam recursos enviando um sinal de volta para o softphone. Não há problema com botões que funcionam localmente no dispositivo.

Limitação

Depois de instalar um dispositivo de áudio no seu cliente, habilitar o redirecionamento de áudio e iniciar uma sessão RDS, os arquivos de áudio podem não reproduzir som. Como solução alternativa, adicione a chave de registro na máquina RDS e, em seguida, reinicie a máquina. Para obter informações, consulte Limitação de áudio na lista de recursos gerenciados através do registro.

Redirecionamento de conteúdo do navegador

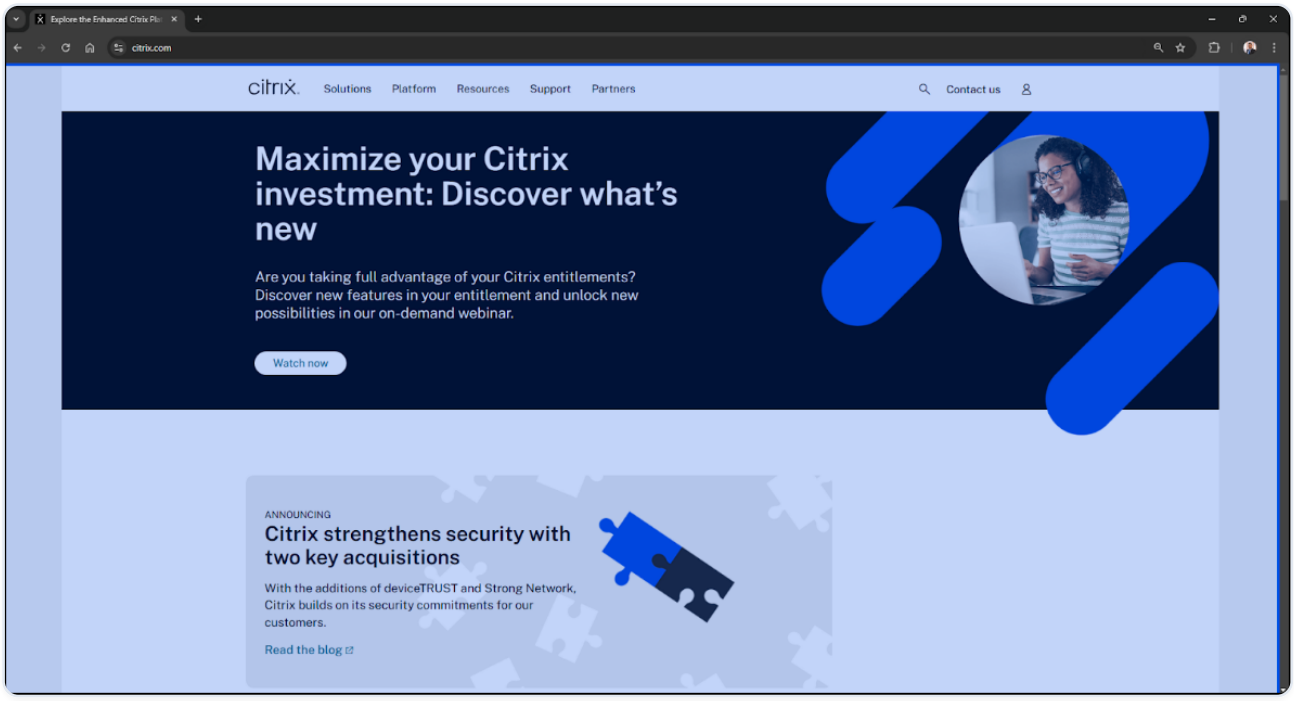
Introdução

O Redirecionamento de Conteúdo do Navegador (BCR) aprimora a experiência do usuário na navegação web em ambientes Citrix Virtual Apps and Desktops™. Ao descarregar a renderização de páginas web para a máquina local do usuário, o BCR reduz a carga do servidor e melhora o desempenho, especialmente para sites complexos ou que consomem muitos recursos.

Como funciona

O BCR utiliza o aplicativo Citrix Workspace™ para criar um ambiente de navegação seguro no dispositivo do usuário. Quando um usuário acessa uma página web permitida, a viewport da janela do navegador é redirecionada para o cliente. O mecanismo do navegador do lado do cliente então aproveita os recursos da máquina local para renderizar a página, resultando em tempos de carregamento mais rápidos e interação mais suave.

Observe que apenas a viewport do navegador é redirecionada. A viewport é a área retangular no seu navegador onde o conteúdo é exibido. A viewport não inclui itens como a Barra de Endereços, Barra de Favoritos ou Barra de Status. Esses itens estão na interface do usuário, que ainda está sendo executada no navegador no VDA.



Principais Benefícios

O redirecionamento de conteúdo do navegador gerencia de forma inteligente o tráfego da web, proporcionando uma experiência superior para seus usuários e reduzindo a carga em sua infraestrutura.

Veja como eles podem beneficiar sua organização:

- **Economia de Custos:** Descarregue páginas web que consomem muitos recursos para os dispositivos dos usuários, liberando recursos valiosos do servidor e reduzindo o consumo de largura de banda. Isso se traduz em custos de hardware e rede mais baixos.
- **Experiência do Usuário Aprimorada:** Ofereça aos seus usuários uma experiência de navegação mais suave e responsiva, mesmo com sites com muitos gráficos. Proporcione um desempenho semelhante ao nativo, eliminando atrasos e melhorando a produtividade.
- **Segurança Aprimorada:** Mantenha um ambiente seguro enquanto permite o acesso a recursos internos e externos.
- **Flexibilidade Aumentada:** Suporte uma ampla gama de casos de uso, desde navegação web básica até aplicativos web complexos que exigem travessia de proxy ou autenticação SSO. Gerencie facilmente as configurações de redirecionamento com controles de política granulares no Citrix Web Studio™

Requisitos do Sistema

Componentes do lado do servidor

Citrix Aplicativos Virtuais e Desktops

- Versão de Serviço de Longo Prazo
  - Requisitos mínimos - Qualquer versão LTSR do Citrix Virtual Apps and Desktops que não esteja no fim da vida útil
  - Recomendado - Citrix Virtual Apps and Desktops 2402 ou superior
- Versão Atual
  - Requisito mínimo - Qualquer versão CR do Citrix Virtual Apps and Desktops que não esteja no fim da vida útil
  - Recomendado - A versão mais recente do Citrix Virtual Apps and Desktops

Componentes do Navegador

- Navegadores
  - Microsoft Edge
  - Google Chrome
- Extensão de redirecionamento de navegador: Publicada nas lojas de aplicativos do Chrome e do Edge
- Recomendamos usar a versão mais recente dos navegadores para a melhor experiência

Componentes do lado do cliente

Windows

- Windows 10 ou 11
- Citrix Workspace App
  - Requisito Mínimo - Qualquer Citrix Workspace App que não esteja no fim da vida útil
  - Recomendado
    - Long Term Service Release - Citrix Workspace App 2402 CU mais recente
    - Versão Atual - Citrix Workspace App 2405 ou superior

Nota:

- O redirecionamento de conteúdo do navegador não é compatível com as versões LTSR 1912 e 2203.1 do Citrix Workspace App para Windows.
- O mecanismo de navegador do lado do cliente necessário para o redirecionamento de conteúdo do navegador é instalado por padrão nas versões atuais do Citrix Workspace App
- O mecanismo de navegador do lado do cliente necessário para o redirecionamento de conteúdo do navegador não é instalado por padrão na versão LTSR 2402 do Citrix Workspace App. Os administradores podem usar o switch ADDLOCAL para instalar os componentes do navegador BCR sobre o Citrix Workspace App.

Para mais detalhes, consulte a documentação do Citrix Workspace App para Windows.

Linux

- Citrix Workspace App
  - Requisito mínimo - Qualquer Citrix Workspace App que não esteja no fim da vida útil
  - Recomendado - Citrix Workspace App 2408 ou superior Para mais detalhes, consulte a documentação Citrix Workspace App Linux

ChromeOS

- Citrix Workspace App
  - Versão mais recente da Chrome Web Store

MacOS

- Citrix Workspace App
  - Requisito Mínimo - Citrix Workspace app 2411 ou superior

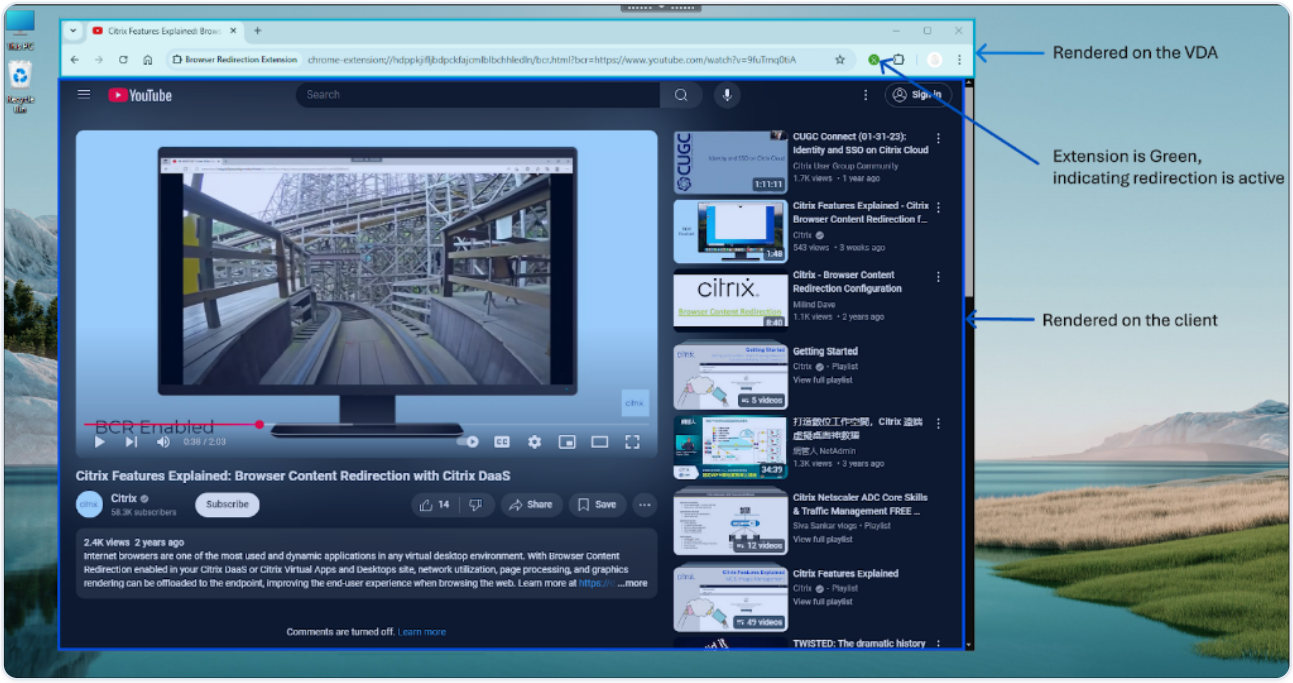
Observação:

- Para MacOS, o pacote de redirecionamento de conteúdo do navegador é independente do Citrix Workspace App e é sempre a versão mais recente. Portanto, o pacote será compatível com várias versões do CWA acima da versão mínima especificada
- Como a dependência do Citrix Workspace App para Mac não existe, a numeração da versão do Redirecionamento de Conteúdo do Navegador não corresponderá à versão do Citrix Workspace App para Mac
- O mecanismo de navegador do lado do cliente não é empacotado com o Citrix Workspace App para Mac. Baixe e instale o lado do cliente para Mac em Citrix Downloads.
- Os pacotes Intel e ARM são separados. Portanto, você precisa instalar a versão apropriada que se adapte ao endpoint MacOS

Etapas para Configurar

1. Instale os componentes do lado do cliente e do lado do servidor de acordo com os requisitos do sistema
    - Para detalhes sobre a implantação da extensão, consulte a seção Implantação da extensão
2. Configurar as políticas do estúdio
    - As políticas do Web Studio oferecem uma maneira granular de configurar o redirecionamento de conteúdo do navegador para atender a uma variedade de casos de uso
    - As políticas básicas permitem que o administrador configure URLs que precisam ser permitidas / não permitidas com o redirecionamento de conteúdo do navegador
    - As URLs podem ser configuradas com curingas
3. Abra um navegador da web compatível e navegar para uma URL permitida
    - Se a correspondência for encontrada na lista de permissões, o site será redirecionado para o cliente
    - O aplicativo Citrix Workspace mescla a janela de visualização no navegador do lado do VDA para uma experiência perfeita
4. A cor do logotipo da extensão especifica o status do redirecionamento de conteúdo

- Verde: Ativo e Conectado
- Cinza: Não ativo / ocioso na guia atual
- Vermelho: Quebrado / Não Funcionando



Nota:

- O redirecionamento de vídeo HTML5 e o redirecionamento de conteúdo do navegador são recursos independentes. As políticas de redirecionamento de vídeo HTML5 não são necessárias para que este recurso funcione. No entanto, o serviço de redirecionamento de vídeo HTML5 Citrix HDX™ é usado para o redirecionamento de conteúdo do navegador.
- Recomendamos fazer todas as configurações através do Web Studio e não com chaves de registro.

Opções de Configuração

O redirecionamento de conteúdo do navegador oferece várias maneiras de configurar para se adequar aos casos de uso de diversos ambientes de clientes. Para obter informações detalhadas sobre as configurações de política, consulte Configurações de política de redirecionamento de conteúdo do navegador.

Mecanismos de redirecionamento

Busca pelo cliente, renderização pelo cliente

Por padrão, o redirecionamento de conteúdo do navegador opera neste modo, ou seja, o mecanismo do navegador do lado do cliente acessa a página da web diretamente. Isso requer o acesso necessário da rede do cliente à página da web. O cenário de busca e renderização pelo cliente descarrega todo o uso de rede, CPU e RAM do Citrix VDA para o cliente e é a maneira mais otimizada de configurar o redirecionamento de conteúdo do navegador.

OPÇÕES DE CONFIGURAÇÃO DE POLÍTICA

- Redirecionamento de conteúdo do navegador: Permitido
- Configuração de ACL de redirecionamento de conteúdo do navegador
    - Especifique os URLs que precisam ser redirecionados. Por padrão, o YouTube é o único site configurado para redirecionamento.
- Configuração da lista de bloqueio de redirecionamento de conteúdo do navegador
    - Opção de configuração opcional para bloquear quaisquer URLs / sub-URLs específicos do redirecionamento. Aproveite esta opção com a anterior para obter a máxima personalização.

Busca pelo servidor, renderização pelo cliente

Neste caso, o mecanismo do navegador do lado do cliente contata e busca conteúdo do servidor web através do VDA usando um canal virtual. Esta opção é útil quando o cliente não tem acesso à internet (por exemplo, thin clients). Baixo consumo de CPU e RAM no VDA, mas a largura de banda é consumida no canal virtual ICA®.

Existem três modos de operação neste cenário. O termo proxy refere-se a um dispositivo proxy que o VDA acessa para obter acesso à Internet.

OPÇÕES DE CONFIGURAÇÃO DE POLÍTICA

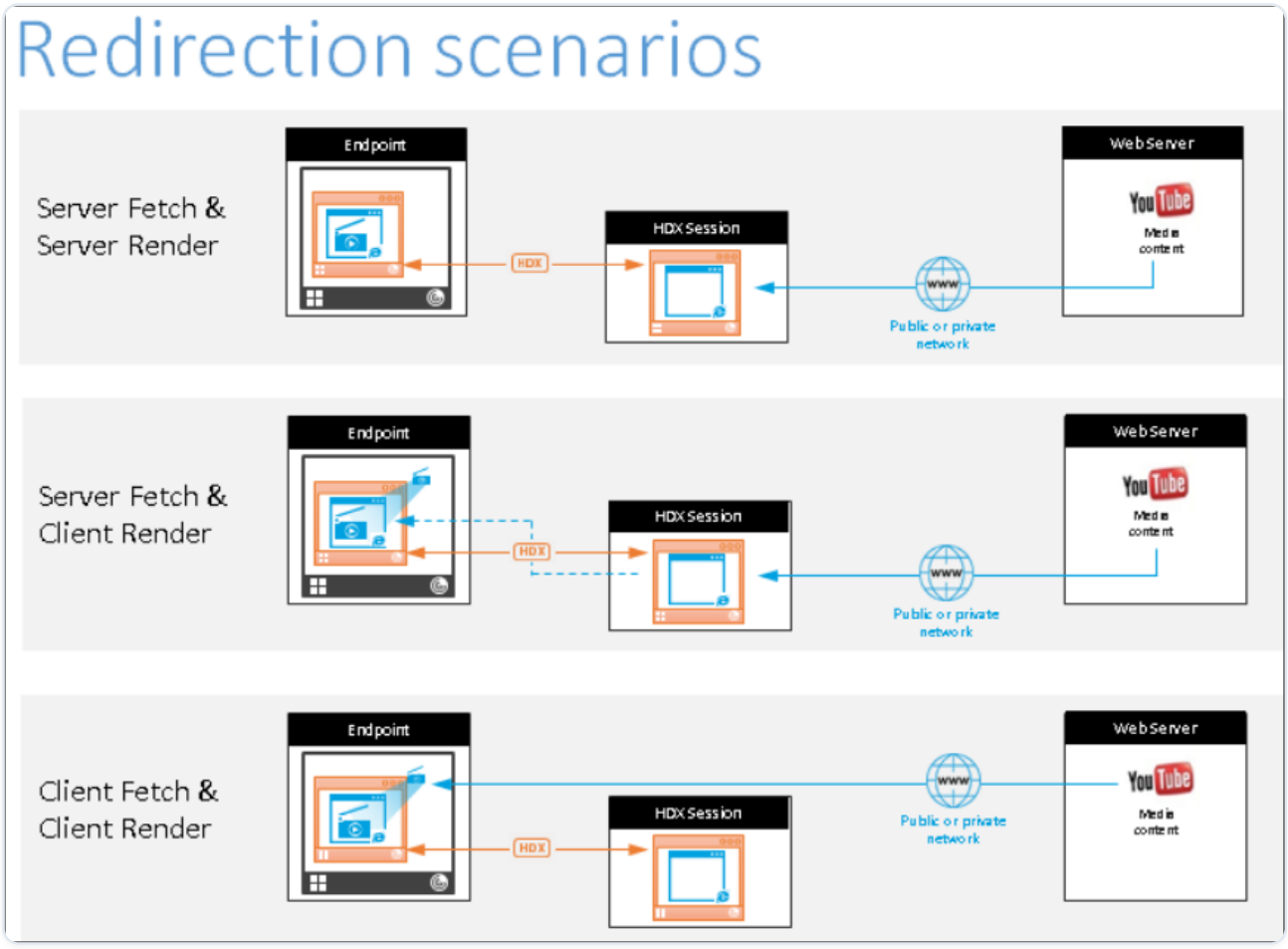
- Além das políticas especificadas na seção Client fetch client render, configure o seguinte
- Configuração de proxy de redirecionamento de conteúdo do navegador
    - **Direto ou Transparente:** Configure isso se você quiser aproveitar a renderização do cliente de busca do servidor e tiver acesso direto ou acesso de proxy transparente à página da web a partir do VDA. A palavra-chave “DIRECT” deve ser configurada na política
    - **Proxy Explícito:** Configure isso se você quiser aproveitar a renderização do cliente de busca do servidor e tiver acesso de proxy explícito à página da web a partir do VDA

- **Arquivos PAC:** Configure isso se você depender de arquivos PAC, os navegadores no VDA podem escolher automaticamente o servidor proxy apropriado para buscar uma URL especificada.

Modo de fallback

Pode haver momentos em que o redirecionamento do cliente falha. Por exemplo, se a máquina cliente não tiver acesso direto à internet, uma resposta de erro pode retornar ao VDA. Nesses casos, o navegador no VDA pode recarregar e renderizar a página no servidor.

Você pode suprimir a renderização de elementos de vídeo no servidor usando a política existente de prevenção de fallback do Windows Media. Defina esta política para Play all content only on client (Reproduzir todo o conteúdo apenas no cliente) ou Play only client-accessible content on client (Reproduzir apenas conteúdo acessível ao cliente no cliente). Essas configurações impedem que elementos de vídeo sejam reproduzidos no servidor se houver falhas no redirecionamento do cliente. Esta política só entra em vigor quando você habilita o redirecionamento de conteúdo do navegador e a política da Lista de Controle de Acesso contém a URL que faz o fallback. A URL não pode estar na política de lista de bloqueio.



Tratamento de autenticação

Sites de autenticação

Na implementação atual do Redirecionamento de Conteúdo do Navegador, independentemente do mecanismo de redirecionamento, os sites de autenticação precisam ser configurados para que o Redirecionamento de Conteúdo do Navegador possa manipular o login em sites.

Exemplo:

1. Quando apenas `<https://www.youtube.com/>`* é configurado na configuração ACL de redirecionamento de conteúdo do navegador e nenhum site de autenticação é configurado, o BCR fará o fallback para a renderização do lado do servidor ao fazer login no site e continuará lá.
2. Neste caso, para que o BCR possa manipular sites de autenticação, configure `<https://www.accounts.google.com/>`* e quaisquer outros sites de autenticação, como o site IdP, conforme necessário. Cada login de site funciona de forma diferente e, portanto, certifique-se de listar
3. Quando configurado, o BCR irá manipular a autenticação. Por exemplo, com a renderização do cliente buscar cliente - a autenticação também ocorrerá a partir do mecanismo do navegador do lado do cliente para uma experiência de login perfeita.

OPÇÕES DE CONFIGURAÇÃO DE POLÍTICA

Configure a política de sites de autenticação de redirecionamento de conteúdo do navegador, além das políticas mencionadas na seção de mecanismos de redirecionamento

> **Nota:**
>
> - O navegador do lado do cliente do BCR não persiste cookies (incluindo autenticação) depois que a janela redirecionada é fechada. Isso se manifestaria como a necessidade de fazer login novamente em sites quando as janelas do BCR são completamente fechadas e reabertas.
> - O navegador do lado do cliente do BCR não lê cookies do navegador do lado do VDA. Consequentemente, a personalização e as preferências do usuário não sincronizam com o navegador do VDA.

Autenticação Integrada do Windows

O redirecionamento de conteúdo do navegador pode fornecer uma maneira perfeita de autenticar em sites quando configurado com a Autenticação Integrada do Windows (IWA) dentro do mesmo domínio do VDA.

OPÇÕES DE CONFIGURAÇÃO DE POLÍTICA

- Configure a política de suporte à Autenticação Integrada do Windows de redirecionamento de conteúdo do navegador

Antes de habilitar o logon único, conclua o seguinte:

- Configure a infraestrutura Kerberos para emitir tickets para nomes de entidade de serviço (SPNs) construídos a partir do nome do host. Por exemplo, HTTP/serverhostname.com.
- Para renderização do cliente buscar servidor: Ao usar o redirecionamento de conteúdo do navegador no modo de busca do servidor, certifique-se de que o DNS esteja configurado corretamente no VDA.
- Para renderização do cliente buscar cliente: Ao usar o redirecionamento de conteúdo do navegador no modo de busca do cliente, certifique-se de que o DNS esteja configurado corretamente no dispositivo cliente e que você permita conexões TCP do overlay para o endereço IP do servidor web.

Autenticação de Proxy

A redireção de conteúdo do navegador pode fornecer uma maneira contínua de autenticar ao seu proxy web ao buscar conteúdo do servidor. Quando ativada, a Redireção de Conteúdo do Navegador obterá e usará automaticamente um tíquete de serviço Kerberos para autenticar com o proxy.

OPÇÕES DE CONFIGURAÇÃO DE POLÍTICA

- Configure a política de autenticação de proxy de busca do servidor de redirecionamento de conteúdo do navegador

Antes de ativar a política de autenticação de proxy de busca do servidor, conclua o seguinte:

- Você precisa configurar seu arquivo PAC para rotear o tráfego através de um proxy web downstream e configurar o proxy para usar autenticação Kerberos

Casos de Uso

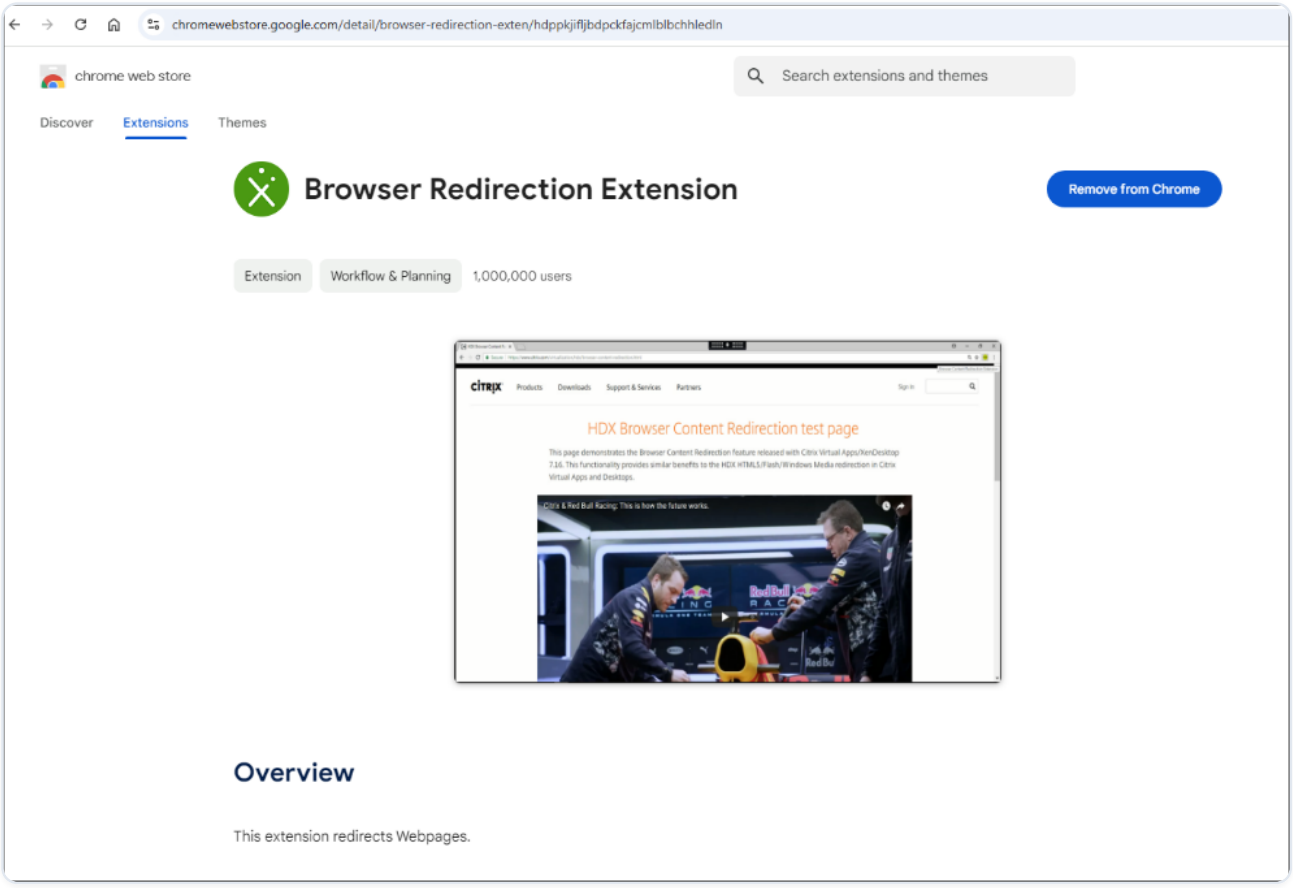
A Redireção de Conteúdo do Navegador (BCR) pode ser utilizada para uma ampla gama de sites, particularmente aqueles que consomem muitos recursos e são frequentemente acessados por

empresas. Isso inclui plataformas de streaming de vídeo como o YouTube, que podem se beneficiar significativamente do descarregamento da renderização para dispositivos de endpoint, reduzindo assim a carga do servidor e economizando custos. Além disso, o BCR é ideal para aplicativos de comunicações unificadas, como ferramentas de videoconferência e colaboração (Google Meet, Teams web, Zoom web) e aplicativos de contact center (Genesys cloud), garantindo desempenho suave e experiência de usuário aprimorada. Ao aproveitar o BCR, as empresas podem otimizar seus recursos e melhorar a eficiência em várias aplicações baseadas na web. Consulte CTX238236 para obter informações sobre como configurar sites específicos.

Implantação da Extensão

Implantar Manualmente

A extensão de redirecionamento do navegador é publicada nas lojas da web do Chrome e Edge. A extensão é necessária apenas no navegador no VDA e não no lado do cliente. Para instalar a extensão, navegar para a webstore do Chrome / Edge, procure pela extensão de redirecionamento do navegador e adicione-a aos respectivos navegadores. Este método funciona para usuários individuais. Para implantar a extensão para um grande grupo de usuários, implante a extensão usando a política de grupo.



Implantar Usando a Política de Grupo

PRÉ-REQUISITOS

- **Acesso:** Você precisará de privilégios de administrador na máquina ou dentro do seu ambiente do Active Directory onde você configurará a Política de Grupo.
- **Arquivos ADMX:** Baixe os arquivos ADMX do Google Chrome (modelos administrativos) para sua versão do Chrome. Você pode encontrá-los na página Ajuda do Google Chrome Enterprise.
- **Modelos do Edge:** Baixe os modelos administrativos do Microsoft Edge (arquivos ADMX) na página (https://learn.microsoft.com/pt-br/deployedge/configure-microsoft-edge#1-download-and-install-the-microsoft-edge-administrative-template) .
- **ID da Extensão e URL de Atualização:** A ID da extensão e a URL de atualização para a extensão de Redirecionamento de Conteúdo do Navegador Citrix.

ETAPAS PARA O GOOGLE CHROME

1. Importar Arquivos ADMX:
    - Copie os arquivos ADMX do Chrome para seu armazenamento central de modelos administrativos. Isso geralmente é %SystemRoot%\PolicyDefinitions no seu controlador de domínio.
2. Abrir Gerenciamento de Política de Grupo:
    - Inicie o Console de Gerenciamento de Política de Grupo (gpmc.msc).
3. Criar ou Editar um GPO:
    - Crie um novo Objeto de Política de Grupo (GPO) ou edite um existente que se aplique aos usuários ou computadores onde você deseja implantar a extensão.
4. navegar até as Configurações de Extensões:
    - No editor de GPO, vá para:
        - Configuração do Usuário > Modelos Administrativos > Modelos Administrativos Clássicos (ADM) > Google > Google Chrome > Extensões
5. Habilite "Configurar a lista de aplicativos e extensões instalados à força":
    - Dê um clique duplo nesta configuração de política e selecione "Ativado".

- Se a configuração Configurar a lista de aplicativos e extensões instalados à força estiver definida como Desativada, a extensão será automaticamente removida do Chrome para todos os usuários.

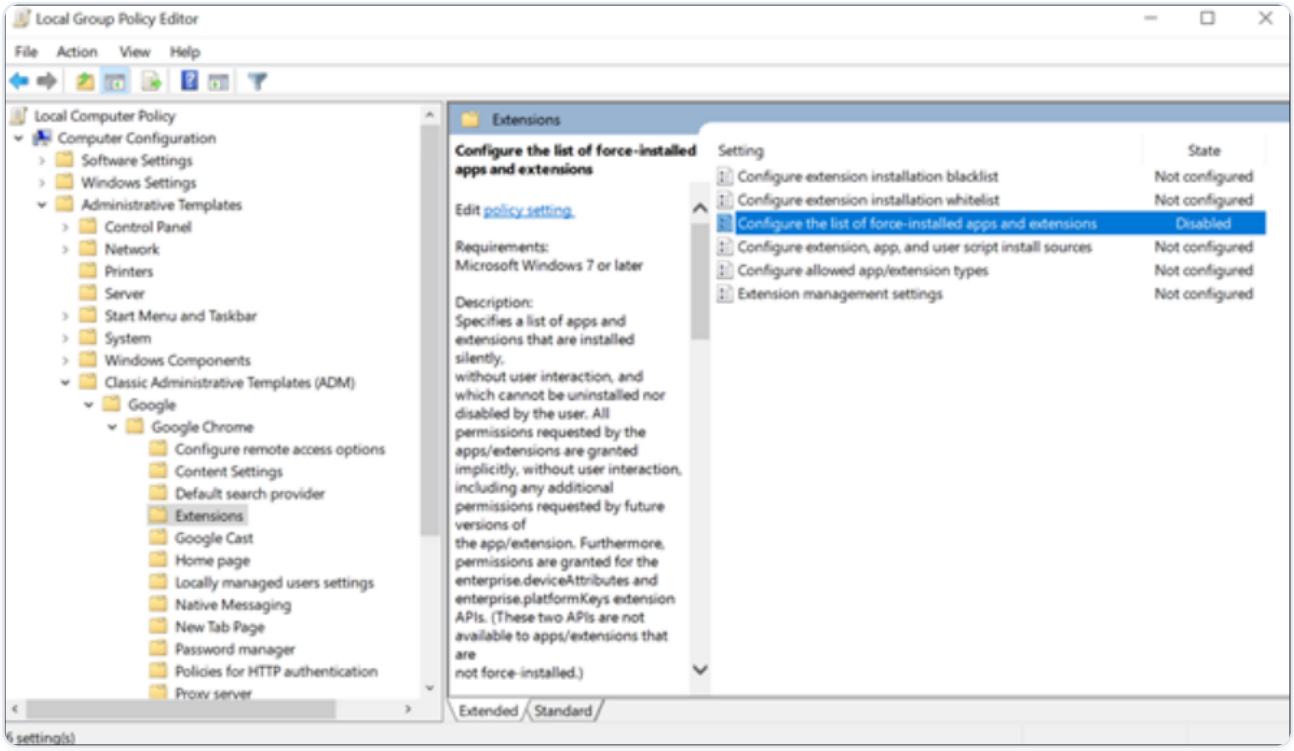
6. Adicionar o ID da Extensão e o URL de Atualização:
   - Clique no botão "Mostrar".
   - Insira o ID da extensão e o URL de atualização no formato: <extension_id>;<update_url>
   - Valor: hdppkjifljbdpckfajcmlblbchhledln; `<https://clients2.google.com/service/update2/crx>` (URL de Atualização)
7. Aplicar o GPO:
   - Vincule o GPO à Unidade Organizacional (OU) apropriada em sua estrutura do Active Directory.
8. Atualizar a Política de Grupo:
   - Nas máquinas de destino, execute gpupdate /force para aplicar a política imediatamente, ou aguarde a política ser atualizada automaticamente.

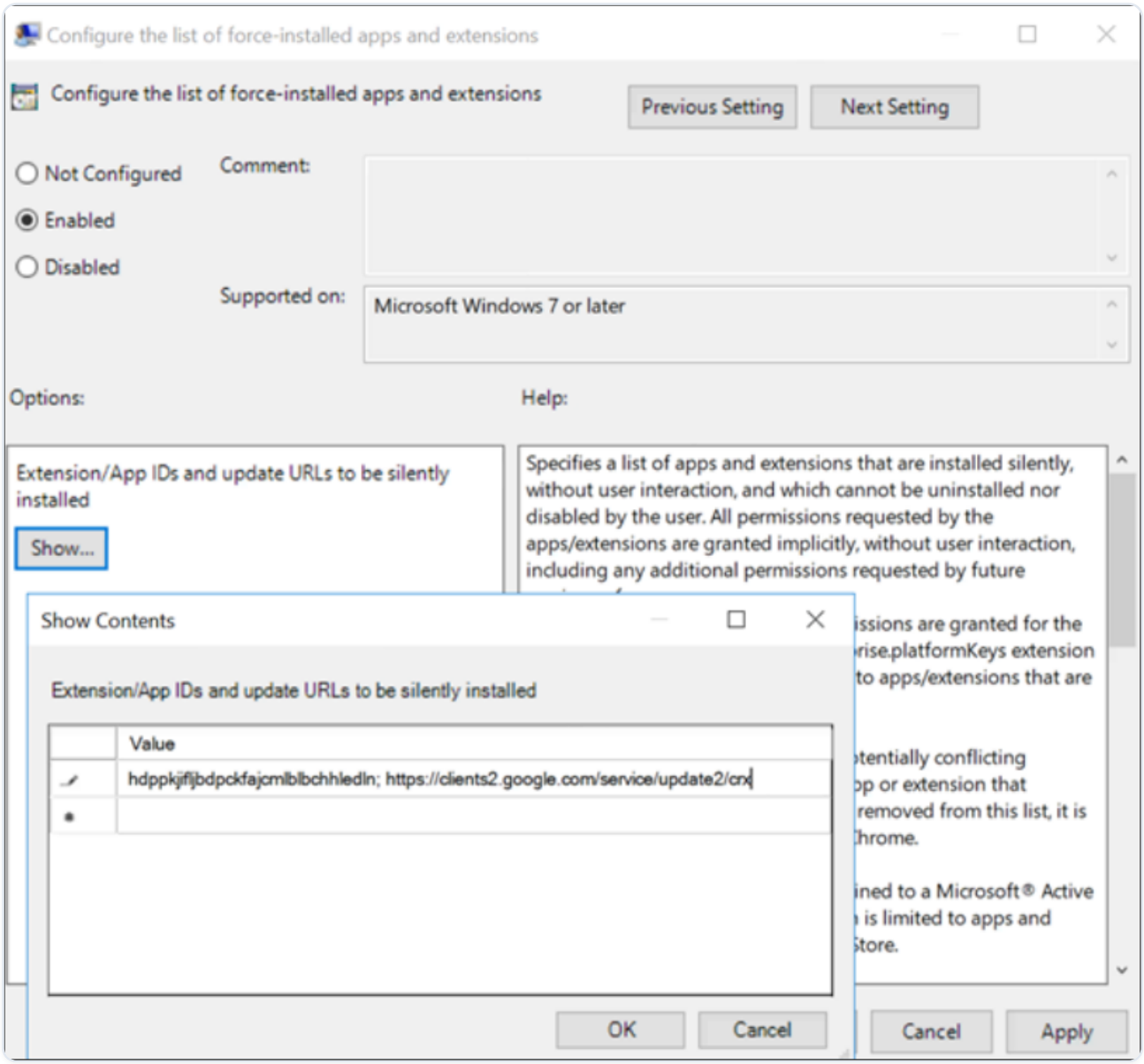
ETAPAS PARA O MICROSOFT EDGE

1. Importar Arquivos ADMX:
   - Copie os arquivos ADMX do Edge para seu armazenamento central de modelos administrativos (%SystemRoot%\PolicyDefinitions).
2. Abrir o Gerenciamento de Política de Grupo:
   - Inicie o Console de Gerenciamento de Política de Grupo (gpmc.msc).
3. Criar ou Editar um GPO:
   - Crie um novo GPO ou edite um existente.
4. navegar para Configurações de Extensões:
   - No editor de GPO, vá para:
     - Configuração do Computador > Políticas > Modelos Administrativos > Microsoft Edge > Extensões
5. Habilitar "Controlar quais extensões são instaladas silenciosamente":

- Clique duas vezes nesta configuração de política e selecione "Habilitado".

6. Adicionar o ID da Extensão e a URL de Atualização:
   - Clique no botão "Mostrar".
   - Insira o ID da extensão e a URL de atualização no formato: <extension_id>;<update_url>
   - Valor: hdppkjifljbdpckfajcmlblbchhledln; `<https://clients2.google.com/service/update2/crx>` (URL de Atualização)
7. Aplicar o GPO:
   - Vincule o GPO à Unidade Organizacional (OU) apropriada em sua estrutura do Active Directory.
8. Atualizar a Política de Grupo:
   - Nas máquinas de destino, execute gpupdate /force ou aguarde a atualização automática.





Solução de problemas

Para obter informações sobre solução de problemas, consulte o artigo da central de conhecimento Como solucionar problemas de redirecionamento de conteúdo do navegador.

Limitações do redirecionamento de conteúdo do navegador

Limitações do lado do servidor (VDA)

O redirecionamento de conteúdo do navegador não pode suportar os seguintes casos de uso. Caso seja necessário um aprimoramento para qualquer um dos cenários mencionados ou novos cenários, entre em contato com a equipe de produto da Citrix.

- Janelas pop-up não são suportadas com o redirecionamento de conteúdo do navegador.
- A persistência de cookies de sessão não é suportada.

- A política de redirecionamento de vídeo HTML5 deve ser desabilitada quando o redirecionamento de conteúdo do navegador estiver em uso.
- Em cenários de desconexão/reconexão de sessão, a janela do navegador VDA precisa ser atualizada para que o BCR seja ativado novamente.
- Impressão e downloads de arquivos de janelas redirecionadas por BCR não são suportados.
- O modo de navegação anônima ou privada não é suportado com o redirecionamento de conteúdo do navegador.

Limitações do lado do cliente (CWA)

- O redirecionamento de conteúdo do navegador não é suportado na estrutura ARMhf
- O BCR suporta um máximo de 25 abas redirecionadas em um navegador e um total combinado de 30 abas redirecionadas em dois navegadores.

Videoconferência HDX™ e compressão de vídeo de webcam

> **Aviso:**
>
> A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

> Webcams podem ser usadas por aplicativos em execução na sessão virtual usando a compressão de vídeo de webcam HDX ou o redirecionamento USB genérico plug-n-play HDX. Use **Citrix Workspace™ app > Preferências > Dispositivos** para alternar entre os modos. A Citrix recomenda que você sempre use a compressão de vídeo de webcam HDX, se possível. O redirecionamento USB genérico HDX é recomendado apenas quando há problemas de compatibilidade de aplicativos com a compressão de vídeo HDX ou quando você precisa de funcionalidades nativas avançadas da webcam. Para melhor desempenho, a Citrix recomenda que o Virtual Delivery Agent tenha pelo menos duas CPUs virtuais.

Para evitar que os usuários alternem da compressão de vídeo de webcam HDX, desative o redirecionamento de dispositivo USB usando as configurações de política em **Configurações de política ICA® > Configurações de política de dispositivos USB**. Os usuários do aplicativo Citrix

Workspace podem substituir o comportamento padrão escolhendo a configuração de Microfone e Webcam do Desktop Viewer **Não usar meu microfone ou webcam**.

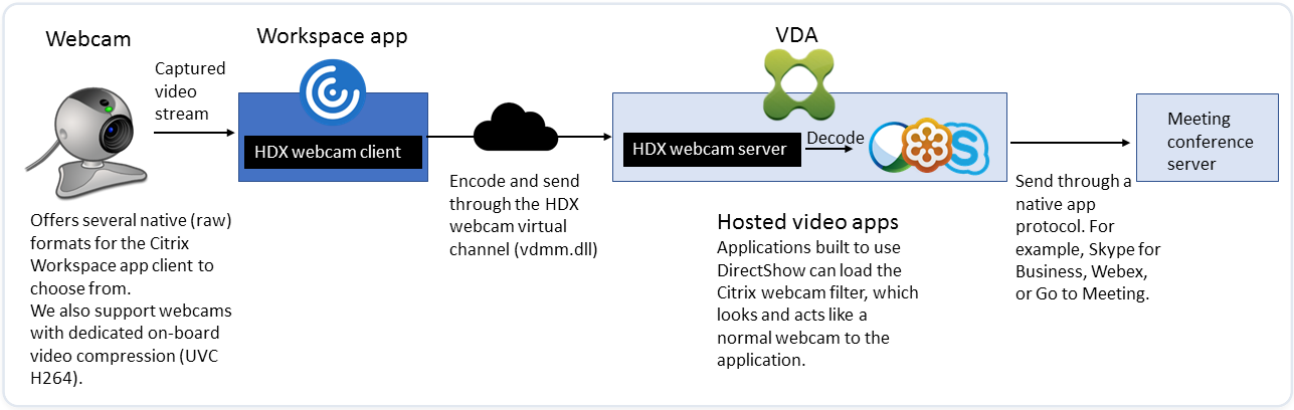
Compressão de vídeo de webcam HDX

A compressão de vídeo de webcam HDX também é chamada de modo de webcam **Otimizado**. Este tipo de compressão de vídeo de webcam envia o vídeo H.264 diretamente para o aplicativo de videoconferência em execução na sessão virtual. Para otimizar os recursos do VDA, a compressão de webcam HDX não codifica, transcodifica e decodifica o vídeo da webcam. Este recurso é ativado por padrão.

Para desativar o streaming de vídeo direto do servidor para o aplicativo de videoconferência, defina a chave do registro como 0 no VDA. Para obter informações, consulte Compressão de vídeo de webcam na lista de recursos gerenciados através do registro.

Se você desativar a funcionalidade padrão para streaming de recursos de vídeo, a compressão de vídeo de webcam HDX usará a tecnologia de estrutura multimídia que faz parte do sistema operacional cliente para interceptar o vídeo de dispositivos de captura, transcodificá-lo e compactá-lo. Os fabricantes de dispositivos de captura fornecem os drivers que se conectam à arquitetura de streaming do kernel do SO.

O cliente lida com a comunicação com a webcam. O cliente então envia o vídeo apenas para o servidor que pode exibi-lo corretamente. O servidor não lida diretamente com a webcam, mas sua integração oferece a mesma experiência em seu desktop. O aplicativo Workspace comprime o vídeo para economizar largura de banda e fornecer melhor resiliência em cenários de WAN.



A compressão de vídeo de webcam HDX exige que as seguintes configurações de política estejam ativadas (todas estão ativadas por padrão).

- Conferência multimídia
- Redirecionamento de Mídia do Windows

Se uma webcam suporta codificação de hardware, a compressão de vídeo HDX usa a codificação de hardware por padrão. A codificação de hardware pode consumir mais largura de banda do que a codificação de software. Para forçar a compressão de software, edite a chave do registro no cliente. Para obter informações, consulte Compressão de software de webcam na lista de recursos gerenciados através do registro.

Requisitos de compressão de vídeo da webcam HDX

A compressão de vídeo da webcam HDX oferece suporte às seguintes versões do aplicativo Citrix Workspace:

PLATAFORMA	PROCESSADOR
Aplicativo Citrix Workspace para Windows	O aplicativo Citrix Workspace para Windows oferece suporte à compressão de vídeo da webcam para aplicativos de 32 e 64 bits no XenApp e XenDesktop 7.17 e posterior. Em versões anteriores, o aplicativo Citrix Workspace para Windows oferece suporte apenas a aplicativos de 32 bits.
Aplicativo Citrix Workspace para Mac	O aplicativo Citrix Workspace para Mac 2006 ou posterior oferece suporte à compressão de vídeo da webcam para aplicativos de 64 bits no XenApp e XenDesktop 7.17 e posterior. Em versões anteriores, o aplicativo Citrix Workspace para Mac oferece suporte apenas a aplicativos de 32 bits.
Aplicativo Citrix Workspace para Linux	O aplicativo Citrix Workspace para Linux oferece suporte apenas a aplicativos de 32 bits na área de trabalho virtual.
Aplicativo Citrix Workspace para Chrome	Como alguns Chromebooks ARM não oferecem suporte à codificação H.264, apenas aplicativos de 32 bits podem usar a compressão de vídeo da webcam HDX otimizada.

Aplicativos de vídeo baseados em Media Foundation oferecem suporte à compressão de vídeo da webcam HDX no Windows 8.x ou superior e Windows Server 2012 R2 e superior. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX132764.

Outros requisitos do dispositivo do usuário:

- Hardware apropriado para produzir som.
- Webcam compatível com DirectShow (use as configurações padrão da webcam). Webcams com capacidade de codificação de hardware reduzem o uso da CPU no lado do cliente.
- Para compressão de vídeo de webcam HDX, instale os drivers da webcam no cliente, obtidos do fabricante da câmera, se possível. A instalação dos drivers do dispositivo não é necessária no servidor.

Diferentes webcams oferecem diferentes taxas de quadros e têm diferentes níveis de brilho e contraste. Ajustar o contraste da webcam pode reduzir significativamente o tráfego de upstream. A Citrix usa as seguintes webcams para validação inicial de recursos:

- Modelos Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- HP Deluxe Webcam

Para ajustar a taxa de quadros de vídeo preferida, edite a chave de registro no cliente. Para obter informações, consulte Taxa de quadros de compressão de vídeo da webcam na lista de recursos gerenciados através do registro.

Streaming de webcam de alta definição

O aplicativo de videoconferência no servidor seleciona o formato e a resolução da webcam com base nos tipos de formato suportados. Quando uma sessão é iniciada, o cliente envia as informações da webcam para o servidor. Escolha uma webcam no aplicativo. Quando a webcam e o aplicativo de videoconferência suportam renderização de alta definição, o aplicativo usa resolução de alta definição. Suportamos resoluções de webcam de até 1920x1080.

Este recurso requer o aplicativo Citrix Workspace para Windows, versão mínima 1808 ou Citrix Receiver para Windows, versão mínima 4.10.

Você pode usar uma chave de registro para desabilitar e habilitar o recurso. Para obter informações, consulte Streaming de webcam de alta definição na lista de recursos gerenciados através do registro.

Se a negociação do tipo de mídia falhar, o HDX retorna à resolução padrão de 352x288 CIF. Você pode usar chaves de registro no cliente para configurar a resolução padrão. Certifique-se de que a câmera suporte a resolução especificada. Para obter informações, consulte Resolução de webcam de alta definição na lista de recursos gerenciados através do registro.

A compressão de vídeo de webcam HDX usa significativamente menos largura de banda em comparação com o redirecionamento USB genérico plug-n-play e funciona bem em conexões WAN. Para ajustar a largura de banda, defina a chave de registro no cliente. Para obter informações, consulte Largura de banda de webcam de alta definição na lista de recursos gerenciados através do registro.

Insira um valor em bits por segundo. Se você não especificar a largura de banda, os aplicativos de videoconferência usarão 350000 bps por padrão.

Redirecionamento USB genérico plug-n-play HDX

O redirecionamento USB genérico plug-n-play HDX (isócrono) também é chamado de modo de webcam **Genérico**. O benefício do redirecionamento USB genérico plug-n-play HDX é que você não precisa instalar drivers em seu thin client/endpoint. A pilha USB é virtualizada de forma que qualquer coisa que você conecte ao cliente local seja enviada para a VM remota. A área de trabalho remota age como se você a tivesse conectado nativamente. A área de trabalho do Windows lida com toda a interação com o hardware e executa a lógica plug-n-play para encontrar os drivers corretos. A maioria das webcams funciona se os drivers existirem no servidor e puderem funcionar via ICA. O modo de webcam genérico usa significativamente mais largura de banda (muitos Megabits por segundo) porque você está enviando vídeo não compactado com protocolo USB pela rede.

Redirecionamento de multimídia HTML5

O redirecionamento de multimídia HTML5 estende os recursos de redirecionamento de multimídia do HDX™ MediaStream para incluir áudio e vídeo HTML5. Devido ao crescimento na distribuição online de conteúdo multimídia, especialmente para dispositivos móveis, a indústria de navegadores desenvolveu maneiras mais eficientes de apresentar áudio e vídeo.

O Flash tem sido o padrão, mas requer um plug-in, não funciona em todos os dispositivos e tem maior consumo de bateria em dispositivos móveis. Empresas como YouTube, NetFlix.com e versões mais recentes de navegadores como Mozilla, Google e Microsoft estão migrando para o HTML5, tornando-o o novo padrão.

A multimídia baseada em HTML5 tem muitas vantagens sobre plug-ins proprietários, incluindo:

- Padrões independentes de empresas (W3C)
- Fluxo de trabalho simplificado de gerenciamento de direitos digitais (DRM)
- Melhor desempenho sem os problemas de segurança levantados pelos plug-ins

Downloads progressivos HTTP

O download progressivo HTTP é um método de pseudo-streaming baseado em HTTP que suporta HTML5. Em um download progressivo, o navegador reproduz um único arquivo (codificado em uma única qualidade) enquanto ele está sendo baixado de um servidor web HTTP. O vídeo é armazenado na unidade à medida que é recebido e é reproduzido a partir da unidade. Se você assistir ao vídeo novamente, o navegador pode carregar o vídeo do cache.

Para um exemplo de download progressivo, consulte a página de teste de redirecionamento de vídeo HTML5. Para inspecionar os elementos de vídeo na página da web e encontrar as fontes (formato de contêiner mp4) nas tags de vídeo HTML5, use as ferramentas de desenvolvedor em seu navegador:

Comparando HTML5 e Flash

RECURSO	HTML5	FLASH
Requer um reprodutor proprietário	Não	Sim
Executa em dispositivos móveis	Sim	Alguns
Velocidade de execução em diferentes plataformas	Alta	Lenta
Compatível com iOS	Sim	Não
Uso de recursos	Menor	Maior
Carrega mais rápido	Sim	Não

Requisitos

Oferecemos suporte apenas ao redirecionamento para downloads progressivos no formato mp4. Não oferecemos suporte a WebM e tecnologias de streaming de taxa de bits adaptável como DASH/HLS.

Oferecemos suporte ao seguinte e usamos políticas para controlá-los. Para obter mais informações, consulte Configurações de política de multimídia.

- Renderização do lado do servidor
- Renderização do cliente com busca do servidor
- Busca e renderização do lado do cliente

Versões mínimas do aplicativo Citrix Workspace™ e do Citrix Receiver™:

- Aplicativo Citrix Workspace 1808 para Windows
- Citrix Receiver para Windows 4.5
- Aplicativo Citrix Workspace 1808 para Linux
- Citrix Receiver para Linux 13.5

VERSÃO MÍNIMA DO NAVEGADOR VDA	VERSÃO/COMPILAÇÃO/SP DO SISTEMA OPERACIONAL WINDOWS
Internet Explorer 11.0	Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Firefox 47 Adicione manualmente os certificados ao armazenamento de certificados do Firefox ou configure o Firefox para procurar certificados em um armazenamento de certificados confiável do Windows. Para obter mais informações, consulte `https://wiki.mozilla.org/CA:AddRootToFirefox`	Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Chrome 51	Windows 10 x86 (1607 RS1) e x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

Componentes da solução de redirecionamento de vídeo HTML5

- **HdxVideo.js** - hook JavaScript que intercepta comandos de vídeo no site. HdxVideo.js se comunica com o WebSocketService usando WebSockets Seguros (SSL/TLS).
- **Certificados SSL de WebSocket**
  - Para a CA (raiz): **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN =

Citrix XenApp/XenDesktop HDX In-Product CA) Localização: Certificados (Computador Local) > Autoridades de Certificação Raiz Confiáveis > Certificados.

- Para a entidade final (folha): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service) Localização: Certificados (Computador Local) > Pessoal > Certificados.

- **WebSocketService.exe** - Executa no sistema local e realiza a terminação SSL e o mapeamento da sessão do usuário. WebSocket Seguro TLS escutando na porta 9001 de 127.0.0.1.
- **WebSocketAgent.exe** - Executa na sessão do usuário e renderiza o vídeo conforme instruído pelos comandos do WebSocketService.

Como faço para habilitar o redirecionamento de vídeo HTML5?

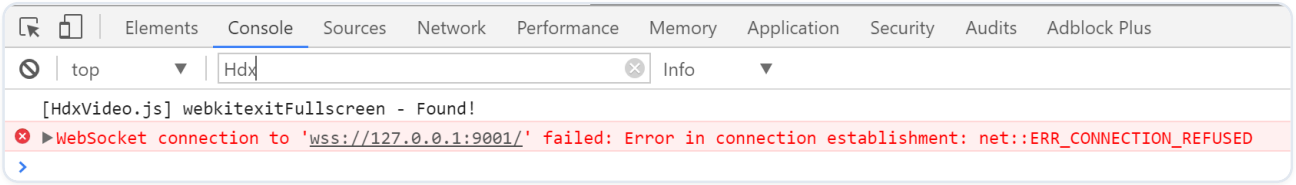
Nesta versão, este recurso está disponível apenas para páginas da web controladas. Requer a adição do JavaScript HdxVideo.js (incluído na mídia de instalação do Citrix Virtual Apps and Desktops) às páginas da web onde o conteúdo multimídia HTML5 está disponível. Por exemplo, vídeos em um site de treinamento interno.

Sites como youtube.com, que são baseados em tecnologias de Adaptive Bitrate (por exemplo, HTTP Live Streaming (HLS) e Dynamic Adaptive Streaming over HTTP (DASH)), não são suportados.

Para obter mais informações, consulte *Configurações de política de multimídia*.

Dicas de Solução de Problemas

Erros podem ocorrer quando a página da web tenta executar HdxVideo.js. Se o JavaScript falhar ao carregar, o mecanismo de redirecionamento HTML5 falha. Certifique-se de que não há erros relacionados a HdxVideo.js inspecionando o console nas janelas da ferramenta de desenvolvedor do seu navegador. Por exemplo:



Otimização para Microsoft Teams (Novo)

A Citrix® oferece suporte a duas maneiras de otimizar o áudio e o vídeo do Microsoft Teams em um ambiente VDI: Otimização Citrix HDX™ e a Nova solução VDI para Teams da Microsoft. O Teams Clássico atingiu o fim da vida útil, portanto, as abordagens de otimização descritas nesta página se aplicam ao cliente atual do Microsoft Teams.

> **Nota:**

> A Microsoft anunciou a descontinuação da Otimização Citrix HDX baseada em WebRTC para Microsoft Teams em endpoints Windows. Dois marcos se aplicam:

> - October 1, 2026 - Fim do Suporte: Não é mais oficialmente suportado pela Microsoft ou Citrix.
> - April 1, 2027 - Fim da Disponibilidade: A otimização baseada em WebRTC para de funcionar. As políticas do Citrix Studio para a otimização legada não terão mais efeito.

> Recomenda-se que os clientes migrem para a Nova solução VDI para Teams. Essa alteração afeta apenas os endpoints Windows. Os endpoints macOS, Linux, ChromeOS e HTML5 não são afetados. Para mais detalhes, consulte Blog da Microsoft.

Abordagens de otimização

- **Otimização Citrix HDX (MTOP)**: Uma solução combinada Citrix e Microsoft que usa um canal virtual de propriedade da Citrix (CTXMTOP). O descarregamento de mídia é tratado por `HdxRtcEngine` no aplicativo Citrix Workspace™. Esta solução é tradicionalmente conhecida como MTOP.
- **Nova solução VDI para Teams**: Uma otimização mais recente que é de propriedade e gerenciada pela Microsoft e usa canais virtuais de propriedade da Microsoft (MSTEAMS, MSTEAM1 e MSTEAM2). Está disponível em endpoints Windows e Mac. Para detalhes completos, consulte Nova solução VDI para Teams na documentação da Microsoft.

Principais distinções

OTIMIZAÇÃO CITRIX HDX	NOVA SOLUÇÃO VDI PARA TEAMS
A otimização é uma solução combinada da Citrix e da Microsoft e usa um canal virtual de propriedade da Citrix (CTXMTOP).	A solução de otimização é de propriedade e gerenciada pela Microsoft e usa canais virtuais de propriedade da Microsoft (MSTEAMS, MSTEAM1 e MSTEAM2).
O descarregamento de mídia é tratado por `HdxRtcEngine` que reside no aplicativo Citrix Workspace.	O descarregamento de mídia é tratado pelo mecanismo de mídia SlimCore em endpoints Windows e Mac.
Nenhum componente adicional é necessário no endpoint, exceto a instalação do aplicativo Citrix Workspace.	Um componente adicional - o **Plugin VDI do Teams** - precisa ser implantado no endpoint por vários meios. Este plug-in gerencia o download e as atualizações do mecanismo de mídia SlimCore.
Disponível nas plataformas de endpoint - Windows, macOS, Linux e ChromeOS.	Disponível nas plataformas de endpoint - Windows e Mac.
Novos recursos são gerenciados em conjunto entre a Citrix e a Microsoft.	Novos recursos são gerenciados pela Microsoft. Os usuários têm acesso a alguns novos recursos indisponíveis com a Otimização Citrix HDX.
Suportado tanto pela Citrix quanto pela Microsoft, dependendo do componente envolvido. Os clientes podem abrir um caso com a Citrix ou com a Microsoft e são redirecionados para a equipe apropriada conforme necessário.	De propriedade e suportado pela Microsoft. A Citrix oferece suporte aos componentes Citrix envolvidos, como o aplicativo Citrix Workspace, a lista de permissões de canais virtuais e os mecanismos de implantação de plug-ins.

Interoperabilidade e roaming

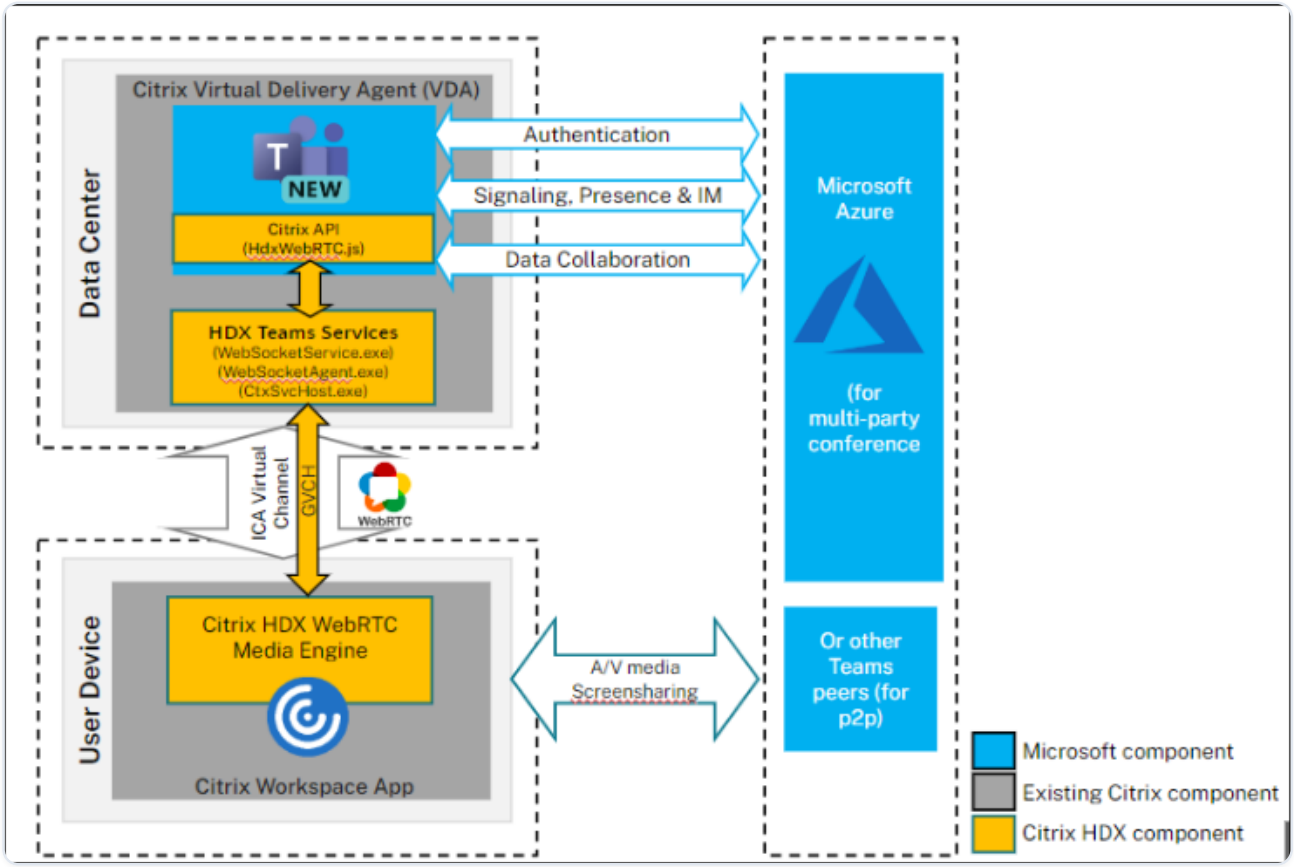
A Otimização Citrix HDX e a nova solução VDI para Teams podem coexistir, mas o cliente Teams usa apenas uma delas por vez.

- A otimização é selecionada quando o aplicativo Teams é iniciado, na seguinte ordem: nova solução VDI para Teams, depois Otimização Citrix HDX (WebRTC), depois redirecionamento padrão de áudio/vídeo.

- Se a nova solução VDI para Teams falhar, o Teams retorna diretamente ao redirecionamento padrão de áudio/vídeo, em vez de WebRTC. É necessário reiniciar o aplicativo Teams para executar novamente a seleção e escolher a otimização adequada.
- O roaming entre endpoints é contínuo e não requer a reinicialização do aplicativo Teams, inclusive quando um usuário faz roaming entre um endpoint que suporta a nova solução VDI para Teams e um que não suporta.

Otimização do Citrix HDX™

No Citrix HDX (Otimização WebRTC), o mecanismo de mídia (HdxRtcEngine) no endpoint responsável pelo tratamento da mídia descarregada está incorporado no aplicativo Citrix Workspace™ e a instalação do aplicativo Citrix Workspace instala automaticamente o mecanismo também.



Requisitos do sistema

Esta seção descreve as versões mínimas e recomendadas necessárias para oferecer suporte ao novo cliente Teams. Observe que, nas versões mínimas, algumas correções de bugs críticas ou os recursos mais recentes podem não estar disponíveis. Implante as versões recomendadas para ter a melhor experiência com as correções e recursos mais recentes.

Sistemas operacionais VDI

Para obter informações detalhadas, consulte as recomendações fornecidas na documentação da Microsoft.

> **Observação:**
>
> - O Windows Server 2016 não é compatível. A Citrix recomenda que você planeje suas atualizações de acordo.
> - Como as versões são atualizadas frequentemente, as versões mencionadas aqui podem se tornar obsoletas (end-of-life). Portanto, consulte as páginas de ciclo de vida do produto do Citrix Workspace app e do Citrix Virtual Apps and Desktops para garantir que você esteja usando versões compatíveis de diferentes componentes.
> - Se você estiver usando o Citrix Virtual Apps and Desktops™ 1912 LTSR, a Citrix recomenda planejar uma atualização, pois ele chegará ao fim da vida útil em dezembro de 2024.

Virtual Delivery Agent (VDA)

VERSÕES MÍNIMAS	VERSÕES RECOMENDADAS
1912 LTSR CU8+; 2203 LTSR (qualquer CU); 2212 CR	2203 LTSR CU5+ (ou) 2402 LTSR e quaisquer versões CR acima

Aplicativo Citrix Workspace

VERSÕES MÍNIMAS	VERSÕES RECOMENDADAS
Windows 2203 LTSR (CU mais recente); Windows 2302 CR; Linux 2207; Mac 2302; Chrome/HTML5 2301	Windows 2402 LTSR; Windows 2405 CR; Linux 2405; Mac 2405; ChromeOS/HTML5 2405

Implantação

1. Instale o novo cliente Teams no VDI. Para obter informações detalhadas, consulte Implantar o novo Teams para VDI.
2. Configure a seguinte chave de registro no VDA para otimizar o novo Teams.
   - **Local**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`

- **Chave (REG_Multi_SZ)**: `ProcessWhitelist`
- **Valor**: `msedgewebview2.exe`

> **Observação:**
>
> A partir do Citrix Virtual Apps and Desktops 2402 LTSR (ou) Citrix Virtual Apps and Desktops 2203 LTSR CU5+, você não precisa configurar manualmente a entrada de registro `msedgewebview2.exe`, pois ela é permitida por padrão.

3. Certifique-se de que a política Redirecionamento do Microsoft Teams esteja habilitada. Esta política está ativada por padrão.
4. Nenhuma configuração adicional é necessária no lado do cliente. Siga as instruções do assistente para instalar o aplicativo Citrix Workspace.

App Layering

O novo Microsoft Teams mudou seu método de instalação e agora é instalado em C:\Program Files\WindowsApps. Para suportar essa mudança, você deve executar o App Layering versão 2403.2 ou posterior. Você pode baixar um disco de atualização na página downloads do App Layering que inclui essa correção.

Para informações detalhadas, consulte a documentação do App Layering.

Citrix Profile Management

Consulte a documentação do Citrix Profile Management para obter informações sobre como habilitar o roaming para o novo Microsoft Teams. A orientação de versão mínima atual para o Citrix Profile Management é 2402 LTSR (ou) 2203 LTSR CU5+.

Considerações de rede

Os requisitos de rede para o novo Teams não diferem do Teams Clássico. Portanto, consulte a seção Requisito de Rede na documentação do Teams Clássico.

Matriz de recursos e suporte de versão

Como as versões são atualizadas frequentemente, algumas versões mais antigas mencionadas aqui podem chegar ao fim da vida útil. Portanto, consulte as páginas de ciclo de vida do produto de Citrix Workspace App e Citrix Virtual Apps and Desktops para garantir que você esteja usando versões suportadas dos diferentes componentes.

Observação:

- As versões mencionadas aqui são as versões mínimas a partir das quais o recurso específico é suportado (ou) a versão mínima na qual o novo Teams é suportado, o que for maior.
- O Citrix Virtual Apps and Desktops 1912 LTSR CU8+ mencionado na seção de versões mínimas não está sendo citado na tabela abaixo, pois atingirá seu fim de vida útil em dezembro de 2024. No entanto, ainda é uma versão suportada até lá.
- Recursos que têm as versões mínimas do Citrix Virtual Apps and Desktops como `N/A` apenas implicam que o recurso não envolveu nenhuma alteração do lado do VDA.

RECURSO	VDA (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA WINDOWS (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA CHROMEOS (VERSÃO MÍNIMA)
Áudio / Vídeo (p2p e conferência)	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR última CU, 2302 CR	2302	2207	2301
Compartilhamento de tela	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR última CU, 2302 CR	2302	2207	2301
i. Borda Vermelha do Indicador de Tela	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não

RECURSO	VDA (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA WINDOWS (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA CHROMEOS (VERSÃO MÍNIMA)
ii. Limitar captura ao Desktop Viewer	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
iii. Vários monitores	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
DTMF	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2301
Suporte a Servidor Proxy	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2305
Compartilhamento de Apps	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2209	Não
Legendas ao Vivo	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
e911 Dinâmico	N/A	2203 LTSR CU mais	2302	2207	2301

RECURSO	VDA (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA WINDOWS (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA CHROMEOS (VERSÃO MÍNIMA)
		recente, 2302 CR			
Conceder Controle	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	Não
Solicitar Controle	N/A	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
Múltiplas Janelas	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
Transcrições de Reunião	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2207	2303
Desfoque de fundo	2203 LTSR (qualquer CU), 2212 CR	2203 LTSR CU mais recente, 2302 CR	2302	2212	2303
Compartilhamento de tela (com Proteção de Aplicativo)	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2309.1 CR	2308	2311	Não

RECURSO	VDA (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA WINDOWS (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA CHROMEOS (VERSÃO MÍNIMA)
Simulcast	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2305 CR	2305	2305	2312
Campainha Secundária	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2307.1 CR	2308	2308	2312
Compartilhar Áudio do Sistema	2203 LTSR (qualquer CU), 2212 CR	2402 LTSR, 2403 CR	2405	2402	Não

Solução de problemas e outras considerações

Para o New Teams, consulte CTX253754, Solucionar problemas do Microsoft Teams. Para as atualizações mais recentes sobre qualquer coisa relacionada ao New Teams, consulte CTX585013.

Limitações conhecidas

Limitações no aplicativo Citrix Workspace

- Suporte HID - Atender e encerrar chamadas não são suportados. Aumentar e diminuir o volume são suportados.
- Os usuários não podem tirar capturas de tela do conteúdo do Microsoft Teams ao usar uma ferramenta de recorte no VDA. No entanto, se uma ferramenta de recorte for usada no lado do cliente, o conteúdo poderá ser capturado.
- Limitações de compartilhamento de áudio do sistema

- O áudio não pode ser compartilhado usando este recurso ao compartilhar a tela com aplicativos ou guias redirecionados RAVE e BCR.
- Este recurso é suportado apenas em desktops publicados

Limitações no VDA

- O New Teams como um aplicativo publicado (seamless) não é suportado
  - Corrigido em CVAD 2402 LTSR, 2203 LTSR CU5 e superior
- Quando você configura a opção High DPI do aplicativo Citrix Workspace para Sim, a janela de vídeo redirecionada aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido para qualquer valor acima de 100%.

Limitações no aplicativo Citrix Workspace e no VDA

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume na máquina cliente – não no VDA.

Para mais detalhes sobre as limitações da Microsoft, consulte Recursos não suportados em VDI.

Nova solução VDI para Teams

> **Nota:**

> A Nova solução VDI para Teams está atualmente geralmente disponível para endpoints Windows e Mac no Citrix®. Esta solução requer uma versão mínima do Microsoft Teams. Consulte Requisitos do sistema.

> Na Nova solução VDI para Teams, a Microsoft usa o SDK do Canal Virtual Citrix para criar canais virtuais personalizados. No endpoint, a mídia é descarregada para o mecanismo de mídia da Microsoft (SlimCore) em vez de `HdxRtcEngine`. Os canais virtuais personalizados transportam a comunicação entre o Teams no VDA e o mecanismo de mídia no endpoint.

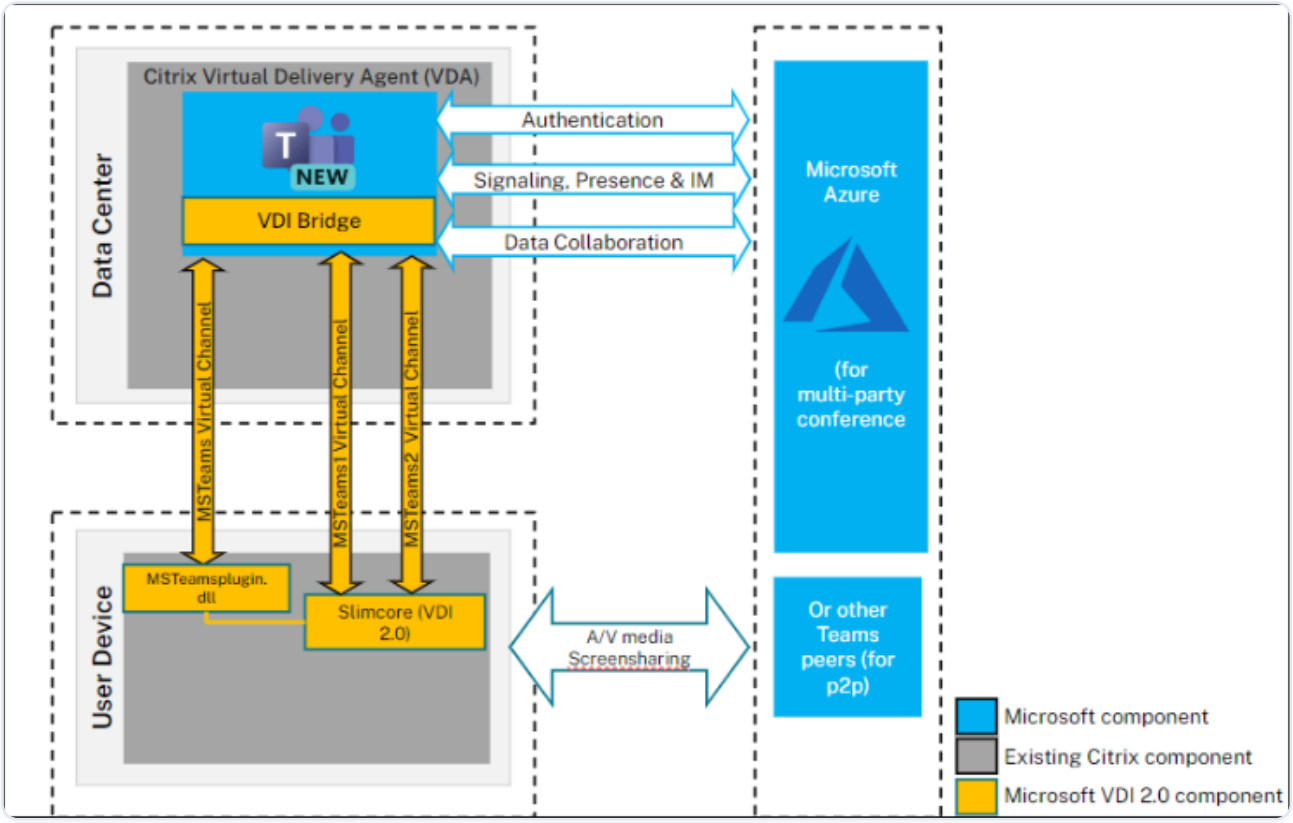
> **Nota:**

> A Microsoft anunciou a descontinuação da Otimização Citrix HDX™ baseada em WebRTC para Microsoft Teams em endpoints Windows. Dois marcos se aplicam:

- October 1, 2026 - Fim do Suporte: Não é mais oficialmente suportado pela Microsoft ou Citrix.
- April 1, 2027 - Fim da Disponibilidade: A otimização baseada em WebRTC para de funcionar. As políticas do Citrix Studio para a otimização legada não terão mais efeito.

Recomenda-se que os clientes migrem para a Nova solução VDI para Teams. Essa alteração afeta apenas os endpoints Windows. Endpoints macOS, Linux, ChromeOS e HTML5 não são afetados. Para mais detalhes, consulte Blog da Microsoft.

Esta solução é de propriedade e gerenciada pela Microsoft. A Citrix oferece suporte aos componentes Citrix envolvidos: o aplicativo Citrix Workspace™, a lista de permissões do canal virtual e os mecanismos de implantação de plug-ins descritos nesta página. Para a arquitetura de propriedade da Microsoft e detalhes completos, consulte Nova solução VDI para Teams na documentação da Microsoft.



Requisitos do sistema

Esta seção lista as versões mínimas e recomendadas necessárias para suportar a Nova solução VDI para Teams. Em versões mínimas, algumas correções de bugs críticas ou os recursos mais

recentes podem não estar disponíveis. Implante as versões recomendadas para a melhor experiência.

Virtual Delivery Agent (VDA)

Nota:

Se você estiver usando 2203 LTSR CU2 ou inferior, ou 2303 CR ou inferior, consulte CTX682593 para entender as limitações nessas versões e planejar sua atualização.

VERSÕES MÍNIMAS	VERSÕES RECOMENDADAS
2203 LTSR CU3; 2305 CR	2203 LTSR CU5+; 2402 LTSR e qualquer CR posterior

Aplicativo Citrix Workspace para Windows

VERSÕES MÍNIMAS	VERSÕES RECOMENDADAS
2203 LTSR (CU mais recente); 2302 CR	2402 LTSR; 2405 CR ou posterior

Aplicativo Citrix Workspace para Mac

VERSÕES MÍNIMAS	VERSÕES RECOMENDADAS
2508.10	2607 ou posterior

Os endpoints Mac exigem macOS 14, 15 ou 26. O macOS 26 exige o aplicativo Citrix Workspace 2511 ou posterior. No aplicativo Citrix Workspace para Mac 2508.10, o plug-in deve ser instalado manualmente. A opção de instalar o plug-in por meio do aplicativo Citrix Workspace, do Client App Management ou do gerenciador de plug-ins de canal virtual está disponível a partir do aplicativo Citrix Workspace para Mac 2603.

Para a versão mínima do Microsoft Teams, requisitos de SO do endpoint e requisitos de hardware, consulte a documentação Microsoft.

Componentes

- Novo Teams `vdiBridge`: o módulo de canal virtual do lado do servidor, empacotado com o Teams.
- Canal virtual personalizado (VC): o VC personalizado de propriedade do Microsoft Teams.
- Plug-in: a DLL do VC do lado do cliente. Responsável pelo download e limpeza do mecanismo de mídia.
- Mecanismo de mídia (SlimCore): o mecanismo de mídia específico do sistema operacional, fornecido pela Microsoft como um pacote MSIX.

Implantação

1. Certifique-se de ter a versão do Microsoft Teams listada em Pré-requisitos.
2. Configure a política **Lista de permissões de canal virtual** para permitir os canais virtuais do Microsoft Teams. Esses canais permitem que o cliente Teams se conecte ao plug-in do lado do cliente. Para obter mais informações, consulte Segurança do canal virtual.

   A solução precisa de três canais virtuais personalizados. Use curingas para permitir o executável `ms-teams.exe` e os canais virtuais personalizados:

   ```
   MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

   MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

   MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
   ```

   Nota:

   - O VDA 2603 e posterior permitem esses três canais virtuais por padrão. Nenhuma configuração de política do Studio é necessária nessas versões.
   - Os curingas para a política de lista de permissões de canal virtual estão disponíveis no CVAD 2203 LTSR CU2 e posterior, ou no Citrix Virtual Apps and Desktops™ 2206 CR e posterior.
   - As máquinas VDA devem ser reiniciadas para que a política entre em vigor.
   - O caminho de instalação do MSTeams muda porque é um aplicativo MSIX, então curingas são necessários. Permita as linhas exatas mostradas acima.

3. Esta solução é controlada por uma política do lado do Microsoft Teams, não por uma política da Citrix. Ela é habilitada por padrão. Para habilitá-la ou desabilitá-la para grupos de usuários específicos, consulte a documentação Microsoft.
4. Implante o plug-in do Teams em seus endpoints. Consulte Opções para instalar o plug-in do Teams.
5. Para o preparo e registro do mecanismo de mídia, e as políticas de grupo que podem bloquear a instalação do MSIX, consulte a documentação Microsoft.

Opções para instalar o plug-in do Teams

Independentemente do método de instalação, o plug-in é colocado no local do aplicativo Citrix Workspace no endpoint:

- Windows (`MsTeamsPluginCitrix.dll`): 64 bits `C:\Program Files (x86)\Citrix\ICA Client`; 32 bits `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

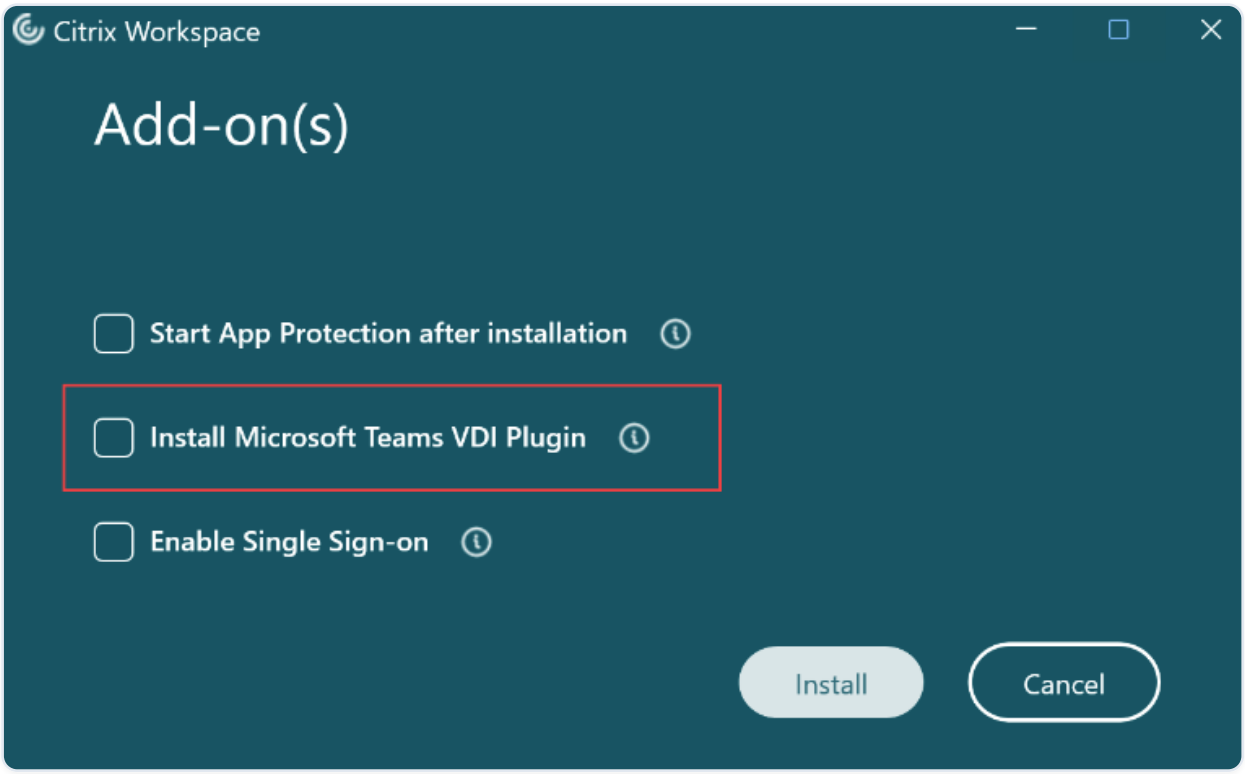
Nota:

- No Windows, instale o aplicativo Citrix Workspace no modo de administrador para que os canais virtuais abram corretamente. A instalação por usuário do aplicativo Citrix Workspace não é suportada.
- O plug-in VDI do Microsoft Teams não é suportado quando o aplicativo Citrix Workspace é instalado da Microsoft Store.
- A instalação do plug-in é interrompida se nenhum aplicativo Citrix Workspace for encontrado no endpoint.
- No Windows, o plug-in e o aplicativo Citrix Workspace devem ter a mesma arquitetura. Um aplicativo Citrix Workspace de 32 bits não pode carregar um plug-in de 64 bits.
- Os plug-ins podem ser atualizados ou reparados, mas não desatualizados, e somente enquanto não houver uma sessão ativa.

Opção 1: Através da instalação do aplicativo Citrix Workspace

- **Windows:** Durante uma instalação nova ou atualização manual, selecione **Instalar Plug-in VDI do Microsoft Teams** na página **Complementos**. A partir do Citrix Workspace app para

Windows 2508, esta opção é selecionada por padrão. Desmarque-a para pular a instalação. As atualizações lembram sua seleção anterior.



Você também pode instalar a partir da linha de comando com a opção `/InstallMSTeamsPlugin`. Por exemplo, `CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y` instala o plug-in, e `/InstallMSTeamsPlugin=N` o impede.

Para uma instalação nova, o mínimo é o Citrix Workspace app para Windows 2402 LTSR. Para atualizações no local, o mínimo é o Citrix Workspace app para Windows 2405 CR. Para obter os detalhes mais recentes, consulte Instalar plug-ins de terceiros.

- **Mac:** A opção de instalar o plug-in durante a instalação do Citrix Workspace app está disponível a partir do Citrix Workspace app para Mac 2603 e requer ação do usuário. O Citrix Workspace app para Mac 2607 instala o plug-in automaticamente por padrão. No Citrix Workspace app para Mac 2508.10, instale o plug-in manualmente. Consulte Opção 2: Baixar o plug-in diretamente.

Opção 2: Baixar o plug-in diretamente

- **Windows:** Baixe o MSI e implante-o com ferramentas como SCCM ou Intune sobre qualquer versão suportada do Citrix Workspace app:
  - Citrix Workspace app de 32 bits: aka.ms/plugin
  - Citrix Workspace app de 64 bits: aka.ms/plugin_x64
  - Citrix Workspace app baseado em Arm: aka.ms/plugin_arm64

- **Mac:** Baixe o plug-in em aka.ms/macplugin e implante-o com ferramentas como JAMF.

Opção 3: Gerenciamento de Aplicativos Cliente (anteriormente serviço de Configuração Global de Aplicativos)

O Gerenciamento de Aplicativos Cliente (anteriormente serviço de Configuração Global de Aplicativos, ou GACS) gerencia as configurações de aplicativos para endpoints gerenciados e não gerenciados, e pode implantar o plug-in do Teams em seus endpoints. No Mac, isso requer o Citrix Workspace app para Mac 2603 ou posterior. Consulte Gerenciamento do plug-in VDI do Microsoft Teams.

Opção 4: Gerenciador de plug-ins de canal virtual

O gerenciador de plug-ins de canal virtual implanta plug-ins em endpoints de cliente para aplicativos que precisam de componentes de endpoint, incluindo a nova solução VDI para Teams. Ele detecta o aplicativo em execução no VDA e solicita ao usuário que instale o plug-in no endpoint. Os administradores podem usá-lo em cenários BYOD. No Mac, isso requer o Citrix Workspace app para Mac 2603 ou posterior. Consulte Gerenciador de plug-ins de canal virtual.

Cenários de atualização de plug-in

A Citrix gerencia as atualizações do plug-in do Teams sem problemas quando o plug-in é instalado pelas Opções 1, 3 ou 4. Se o plug-in for instalado manualmente (Opção 2), a Citrix não manipular as atualizações.

- Certifique-se de que a atualização automática do aplicativo Citrix Workspace esteja ativada para atualizações automáticas de plug-in.
- Garanta um mínimo de Citrix Workspace app para Windows 2405. O Citrix Workspace app para Windows 2508 ou posterior instala o plug-in automaticamente quando o Citrix Workspace app é atualizado automaticamente.
- A Citrix não manipular a desinstalação do plug-in. Desinstale o plug-in separadamente quando necessário.

> **Nota:**
>
> A Citrix gerencia as atualizações do plug-in do Teams, não do mecanismo de mídia. A Microsoft fornece e atualiza o mecanismo de mídia.

Teams como um aplicativo publicado da Citrix

O Teams publicado como um aplicativo Citrix Virtual Apps pode ser otimizado com esta solução quando todos os componentes necessários atenderem às versões mínimas. Para as versões necessárias e limitações conhecidas, consulte a documentação Microsoft.

Interoperabilidade e roaming

Consulte Otimização para Microsoft Teams para saber como a nova solução VDI para Teams e a Otimização Citrix HDX interagem e como o roaming se comporta.

Considerações de rede

Consulte Considerações de rede na documentação da Microsoft.

Suporte a recursos

O conjunto de recursos e a implementação são de propriedade da Microsoft. Consulte a lista de recursos na documentação da Microsoft.

Solução de problemas

O cliente do Microsoft Teams relata o status de otimização e, quando a otimização falha, um código de erro. Esses indicadores de status e códigos de erro são definidos pela Microsoft. Para a lista completa e solução de problemas de ponta a ponta, consulte Solução de problemas da nova solução VDI para Teams na documentação da Microsoft.

O Citrix Monitor oferece visibilidade do estado de otimização desta solução. Nos detalhes de uma sessão, a exibição Topologia da Sessão mostra se o aplicativo está otimizado e sinaliza quaisquer componentes ausentes, como o gerenciador de plug-ins, o plug-in e sua versão, o estado do canal virtual e o status da lista de permissões do canal virtual. Para obter mais informações, consulte Visibilidade da otimização de comunicações em tempo real.

Alguns códigos de erro da Microsoft apontam para a configuração do lado da Citrix. Verificações comuns da Citrix:

- Se o cliente do Teams relatar que os canais virtuais personalizados estão bloqueados (erro da Microsoft 2003), confirme se a lista de permissões do canal virtual inclui MSTEAMS, MSTEAM1 e MSTEAM2.
- Se o cliente do Teams relatar que nenhum plug-in foi detectado (erro da Microsoft 2000), confirme se o plug-in está instalado e carregado. No Process Explorer, selecione `wfica32.exe`, mostre o painel inferior e verifique a guia DLL para `MsTeamsPluginCitrix.dll`.

- Se o cliente do Teams relatar uma versão não suportada do aplicativo Citrix Workspace (erro da Microsoft 2004), atualize para uma versão suportada. Consulte Requisitos do sistema.

Limitações conhecidas

Os recursos e a implementação são de propriedade da Microsoft. Consulte Problemas conhecidos na documentação da Microsoft.

Otimização para Microsoft Teams (Clássico)

> **Nota:**

> O novo Microsoft Teams 2.1 agora está geralmente disponível para VDA. Esta versão do Microsoft Teams é compatível com a Otimização do Citrix Microsoft Teams usando WebRTC (VDI 1.0).

> Se você estiver usando o Citrix Virtual Apps and Desktops 2402, não precisará configurar manualmente a entrada de registro `msedgewebview2.exe`, pois ela está na lista de permissões por padrão.

> Os aplicativos publicados agora são compatíveis com o novo Microsoft Teams.

> Se você estiver usando o Citrix Virtual Apps and Desktops 2311 ou anterior, uma nova configuração de registro será necessária no VDA para permitir que o novo Microsoft Teams acesse o canal virtual do Citrix. Para habilitar a otimização do Microsoft Teams 2.1, configure a seguinte chave de registro no VDA:

> **Local**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`

> **Chave** (REG_Multi_SZ): `ProcessWhitelist`

> **Valor**: `msedgewebview2.exe`

> Para obter mais informações, consulte a documentação Microsoft.

> A Citrix oferece otimização para Microsoft Teams baseado em desktop usando Citrix Virtual Apps and Desktops™ e o aplicativo Citrix Workspace™. Por padrão, agrupamos todos os componentes necessários no aplicativo Citrix Workspace e no Virtual Delivery Agent (VDA).

Nossa otimização para Microsoft Teams inclui serviços HDX™ do lado do VDA e uma API para interface com o aplicativo hospedado do Microsoft Teams para receber comandos. Esses componentes abrem um canal virtual de controle (CTXMTOP) para o mecanismo de mídia do lado do aplicativo Citrix Workspace. O endpoint decodifica e fornece o multimídia localmente, movendo a janela do aplicativo Citrix Workspace de volta para o aplicativo Microsoft Teams hospedado.

A autenticação e a sinalização ocorrem nativamente no aplicativo hospedado do Microsoft Teams, assim como os outros serviços do Microsoft Teams (por exemplo, chat ou colaboração). O redirecionamento de áudio/vídeo não os afeta.

O `CTXMTOP` é um canal virtual de comando e controle. Isso significa que a mídia não é trocada entre o aplicativo Citrix Workspace e o VDA.

Apenas client-fetch/client-render está disponível.

Esta demonstração em vídeo lhe dá uma ideia de como o Microsoft Teams funciona em um ambiente virtual Citrix.



Instalação do Microsoft Teams

A Citrix e a Microsoft recomendam a versão mais recente disponível do Microsoft Teams e que ela seja mantida atualizada. As versões do aplicativo de desktop do Microsoft Teams com datas de lançamento mais de 90 dias anteriores à data de lançamento da versão atual não são suportadas. As versões não suportadas do aplicativo de desktop do Microsoft Teams exibem uma página de bloqueio para os usuários e solicitam a atualização do aplicativo.

Para obter informações sobre as versões mais recentes disponíveis, consulte Histórico de atualizações do aplicativo Teams (Desktop e Mac).

Recomendamos que você siga as diretrizes de instalação do Microsoft Teams para toda a máquina. Além disso, evite usar o instalador .exe que instala o Microsoft Teams em `AppData`. Em vez disso, instale em `C:\Program Files (x86)\Microsoft\Teams` usando o sinalizador `ALLUSER=1` da linha de comando.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

Este exemplo também usa o parâmetro `ALLUSERS=1`. Ao definir este parâmetro, o Instalador do Microsoft Teams para toda a máquina aparece em **Programas e Recursos** no **Painel de Controle**. Além disso, em **Aplicativos e recursos** nas Configurações do Windows para todos os usuários do computador. Todos os usuários podem então desinstalar o Microsoft Teams se tiverem credenciais de administrador.

É importante entender a diferença entre `ALLUSERS=1` e `ALLUSER=1`. Você pode usar o parâmetro `ALLUSERS=1` em ambientes não-VDI e VDI. Use o parâmetro `ALLUSER=1` apenas em ambientes VDI para especificar uma instalação por máquina.

No modo `ALLUSER=1`, o aplicativo Microsoft Teams não se atualiza automaticamente sempre que há uma nova versão. Recomendamos este modo para ambientes não persistentes, como aplicativos compartilhados hospedados ou desktops de um Windows Server ou catálogos aleatórios/agrupados do Windows 10. Para obter mais informações, consulte Instalar o Microsoft Teams usando MSI (seção Instalação VDI).

Suponha que você tenha ambientes VDI persistentes dedicados do Windows 10. Você deseja que o aplicativo Microsoft Teams se atualize automaticamente e prefere que o Microsoft Teams seja instalado por usuário em `Appdata/Local`. Neste caso, use o instalador `.exe` ou o MSI sem `ALLUSER=1`.

> **Nota:**
>
> Recomendamos instalar o VDA antes de instalar o Microsoft Teams na imagem dourada. Esta ordem de instalação é necessária para que o sinalizador `ALLUSER=1` tenha efeito. Se você instalou o Microsoft Teams na máquina virtual antes de instalar o VDA, desinstale e reinstale o Microsoft Teams.

Para Acesso Remoto a PC

Recomendamos que você instale o Microsoft Teams versão 1.4.00.22472 ou posterior após a instalação do VDA. Caso contrário, você precisará sair e entrar novamente para que o Microsoft Teams detecte o VDA conforme o esperado. A versão 1.4.00.22472 e posteriores incluem lógica aumentada executada no momento do lançamento do Microsoft Teams e no momento do login para detecção do VDA. Essas versões também incluem identificação do tipo de sessão ativa (HDX, RDP ou conectado localmente à máquina cliente). Se você estiver conectado localmente, versões anteriores do Microsoft Teams podem falhar ao detectar e desabilitar certos recursos ou

elementos da interface do usuário. Por exemplo, Salas de Reunião, janelas pop-out para reuniões e bate-papo, ou reações de reunião.

> **Importante:**
>
> Ao alternar de uma sessão local para uma sessão HDX e se o Microsoft Teams for mantido aberto e em execução em segundo plano, você deve sair e reiniciar o Microsoft Teams para otimizar corretamente com o HDX. Por outro lado, se você usar o Microsoft Teams remotamente por meio de uma sessão HDX otimizada, desconecte a sessão HDX e reconecte-se à mesma sessão do Windows localmente no dispositivo. Ao trabalhar no escritório, você deve reiniciar o Microsoft Teams para que ele possa detectar corretamente o estado do PC Remoto (HDX ou local). Isso ocorre porque o Microsoft Teams só pode avaliar o modo VDI no momento do lançamento do aplicativo, e não enquanto já está em execução em segundo plano. Sem uma reinicialização, o Microsoft Teams pode falhar ao carregar recursos como janelas pop-out, Salas de Reunião ou reações de reunião.

Para App Layering

Se estiver usando o Citrix App Layering para gerenciar instalações de VDA e Microsoft Teams em diferentes camadas, você deve criar uma nova chave de registro nos VDAs do Windows antes de instalar o Microsoft Teams com o sinalizador `ALLUSER=1` da linha de comando. Para obter mais informações, consulte a seção *Otimização para Microsoft Teams com Citrix App Layering* em Multimídia.

Recomendações de Gerenciamento de Perfil

Recomendamos usar o instalador para toda a máquina para ambientes Windows Server e VDI agrupado do Windows 10.

Quando o sinalizador **ALLUSER=1** é passado para o MSI a partir da linha de comando (o instalador para toda a máquina), o aplicativo Microsoft Teams é instalado em `C:\Program Files (x86)` (~300 MB). O aplicativo usa `AppData\Local\Microsoft\TeamsMeetingAddin` para logs e `AppData\Roaming\Microsoft\Teams` (~600–700 MB) para configurações específicas do usuário, cache de elementos na interface do usuário e assim por diante.

> **Importante:**

> Se você não passar o sinalizador **ALLUSER=1**, o MSI coloca o instalador Teams.exe e `setup.json` em `C:\Program Files (x86)\Teams Installer`. Uma chave de registro (TeamsMachineInstaller) é adicionada em: `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`

> Um logon de usuário subsequente aciona a instalação final em **AppData**.

Instalador para toda a máquina

A seguir, um exemplo de pastas, atalhos da área de trabalho e registros criados pela instalação do instalador para toda a máquina do Microsoft Teams em uma VM Windows Server 2016 de 64 bits:

Pasta:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Atalho da Área de Trabalho:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

Registro:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Nome: `Teams`
- Tipo: `REG_SZ`
- Valor: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Nota:**

> O local do registro varia de acordo com os Sistemas Operacionais subjacentes e a arquitetura (bitness).

Recomendações

- Recomendamos desativar a inicialização automática excluindo as chaves de registro do Microsoft Teams. Isso evita que muitos logons que ocorrem ao mesmo tempo (por exemplo, no início do seu dia de trabalho) aumentem o uso da CPU da VM.
- Se a área de trabalho virtual não tiver uma GPU/vGPU, recomendamos definir **Desativar aceleração de hardware da GPU** nas **Configurações** do Microsoft Teams para melhorar o desempenho. Essa configuração (`"disableGpu":true`) é armazenada em `%Appdata%\Microsoft\Teams` em `desktop-config.json`. Você pode usar um script de logon para editar esse arquivo e definir o valor como **true**.
- Se estiver usando o Citrix Workspace Environment Management™ (WEM), ative a **Proteção contra Picos de CPU** para gerenciar o consumo do processador para o Microsoft Teams.

Instalador por usuário

Ao usar o instalador `.exe`, o processo de instalação difere. Todos os arquivos são colocados em AppData.

Pasta:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Atalho na área de trabalho:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

Registro:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

Melhores Práticas

As recomendações de melhores práticas são baseadas nos cenários de caso de uso. Usar o Microsoft Teams com uma configuração não persistente requer um gerenciador de cache de perfil para uma sincronização eficiente dos dados de tempo de execução do Microsoft Teams. Com um gerenciador de cache de perfil, as informações específicas do usuário apropriadas são

armazenadas em cache durante a sessão do usuário. Por exemplo, as informações específicas do usuário incluem dados do usuário, perfil e configurações. Sincronize os dados nestas duas pastas:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

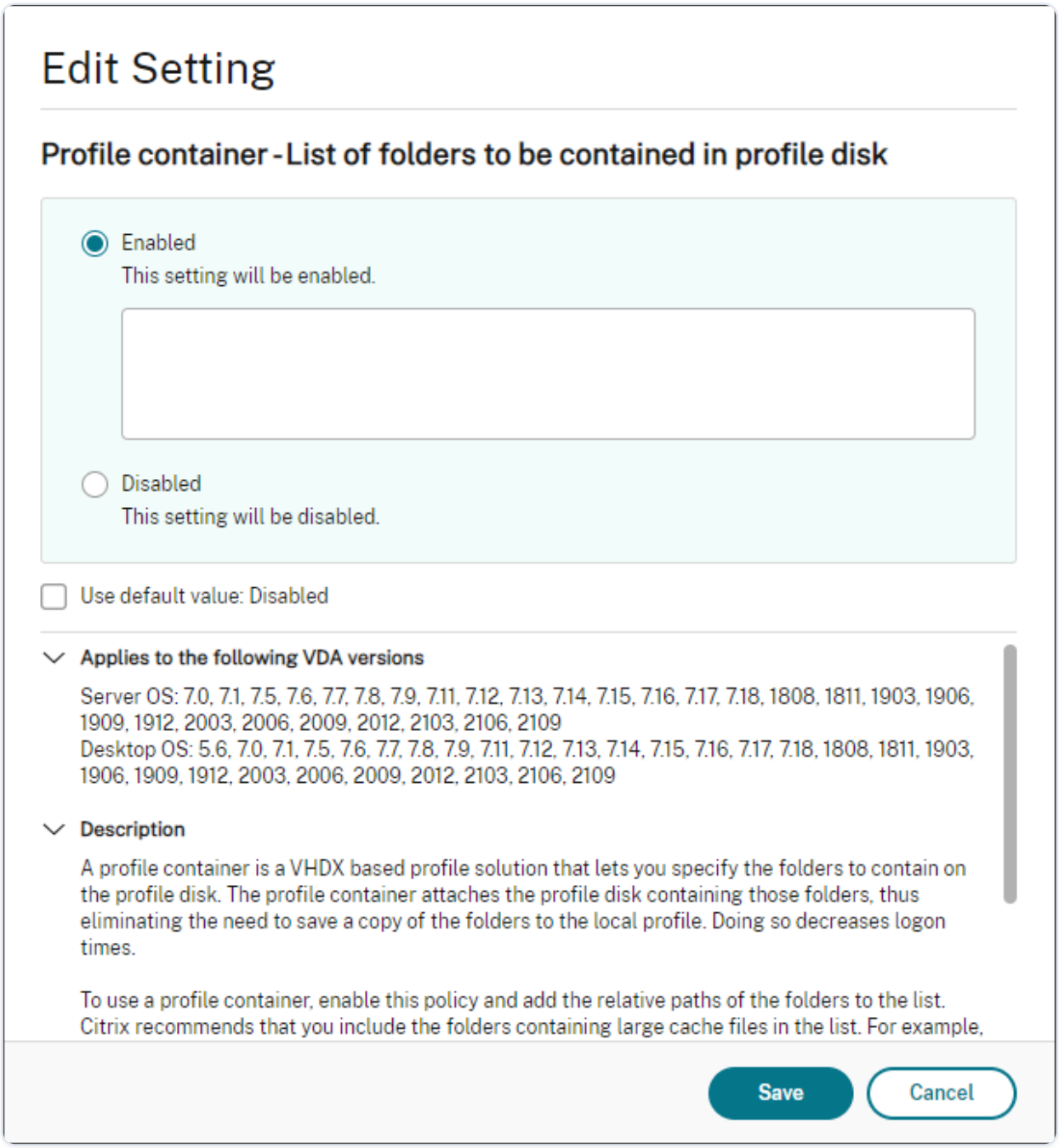
Lista de exclusão de conteúdo em cache do Microsoft Teams para configuração não persistente

Exclua os arquivos e diretórios da pasta de cache do Microsoft Teams conforme descrito na documentação Microsoft. Essa ação ajuda a reduzir o tamanho do cache do usuário para otimizar ainda mais sua configuração não persistente.

Caso de uso: cenário de sessão única

Nesse cenário, o usuário final usa o Microsoft Teams em um local por vez. Eles não precisam executar o Microsoft Teams em duas sessões do Windows ao mesmo tempo. Em uma implantação comum de desktop virtual, cada usuário é atribuído a um desktop, e o Microsoft Teams é implantado no desktop virtual como um aplicativo. Recomendamos habilitar o contêiner de perfil do Citrix e redirecionar os diretórios por usuário listados em Instalador por usuário para o contêiner.

1. Implante o instalador do Microsoft Teams para toda a máquina (**ALLUSER=1**) na imagem dourada.
2. Habilite o Citrix Profile Management e configure o armazenamento de perfil de usuário com as permissões adequadas.
3. Habilite a seguinte configuração de política do Profile Management: **Sistema de arquivos > Sincronização > Contêiner de perfil – Lista de pastas a serem contidas no disco de perfil**.



Liste todos os diretórios por usuário nesta configuração. Você também pode configurar essas definições usando o serviço Citrix Workspace Environment Management (WEM).

4. Aplique as configurações ao grupo de entrega correto.
5. Faça login para validar a implantação.

Requisitos do sistema

Versão mínima recomendada - Delivery Controller (DDCs) 1906.2

Se você estiver usando uma versão anterior, consulte Habilitar otimização do Microsoft Teams:

Sistemas operacionais suportados:

- Windows Server 2022, 2019, 2016, 2012R2 Standard e edições de data center, e com a opção Server Core

Versão mínima - Virtual Delivery Agents (VDAs) 1906.2

Sistemas operacionais suportados:

- Windows 11.
- Windows 10 de 64 bits, versões 1607 e posteriores. Aplicativos hospedados em VM são suportados no Citrix Workspace app para Windows 2109.1 e posterior.
- Windows Server 2022, 2019, 2016 e 2012 R2 (edições Standard e data center).

Requisitos:

- BCR_x64.msi - o MSI que inclui o código de otimização do Microsoft Teams e inicia automaticamente a partir da GUI. Se você estiver usando a interface de linha de comando para a instalação do VDA, não o exclua.

Versão recomendada – Citrix Workspace app para Windows CR mais recente e Versão mínima - Citrix Workspace app 1907 para Windows

- Windows 11.
- Windows 10 (edições de 32 e 64 bits, incluindo edições Embedded) (O suporte para Windows 7 foi interrompido na Versão 2006) (O suporte para Windows 8.1 foi interrompido na versão 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) e 2019 LTSC (v1809).
- Arquiteturas de processador (CPU) suportadas: x86 e x64 (ARM não é suportado).
- Requisito de endpoint: CPU dual core de aproximadamente 2,2–2,4 GHz que pode suportar resolução HD de 720p durante uma chamada de videoconferência ponto a ponto.
- CPUs dual ou quad-core com velocidades base mais baixas (~1,5 GHz) equipadas com Intel Turbo Boost ou AMD Turbo Core que podem aumentar até pelo menos 2,4 GHz.
- Thin Clients HP verificados: t630/t640, t730/t740, mt44/mt45.
- Thin Clients Dell verificados: 5070, 5470 Mobile TC e AIO.
- Thin Clients 10ZiG verificados: 4510 e 5810q.
- Para obter uma lista completa de endpoints verificados, consulte Thin Clients.
- O aplicativo Citrix Workspace requer pelo menos 600 MB de espaço livre em disco e 1 GB de RAM.

- O requisito mínimo do Microsoft .NET Framework é a versão 4.8. O aplicativo Citrix Workspace baixa e instala automaticamente o .NET Framework se ele não estiver presente no sistema.

Os administradores podem habilitar/desabilitar o Microsoft Teams iniciando no modo otimizado alterando a política de otimização do Teams. Os usuários que iniciam no modo otimizado no aplicativo Citrix Workspace não podem desabilitar o Microsoft Teams.

Versão mínima - aplicativo Citrix Workspace 2006 para Linux

Software:

- `GStreamer` 1.0 ou posterior ou Cairo 2
- libc++-9.0 ou posterior
- `libgdk` 3.22 ou posterior
- OpenSSL 1.1.1d
- Distribuição Linux x64

Hardware:

- CPU dual-core de no mínimo 1,8 GHz que suporte resolução HD de 720p durante uma chamada de videoconferência ponto a ponto
- CPU dual ou quad-core com velocidade base de 1,8 GHz e alta velocidade Intel Turbo Boost de pelo menos 2,9 GHz

Para obter uma lista completa de endpoints verificados, consulte Thin Clients.

Para obter mais informações, consulte Pré-requisitos para instalar o aplicativo Citrix Workspace.

Você pode desabilitar a otimização do Microsoft Teams atualizando o valor do campo **VDWEBRTC** para Off no arquivo `/opt/Citrix/ICAClient/config/module.ini`. O padrão é VDWEBRTC=On. Após a conclusão da atualização, reinicie a Sessão. (É necessária permissão de root).

Versão mínima - aplicativo Citrix Workspace 2012 para Mac

Sistemas operacionais suportados:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 e posterior.
- macOS Monterey.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída)

> **Nota:**

> O aplicativo Citrix Viewer requer acesso às preferências de Segurança e Privacidade do macOS para que o compartilhamento de tela funcione. Os usuários configuram essa preferência em **Menu Apple > Preferências do Sistema > Segurança e Privacidade > Guia Privacidade > Gravação de tela** e selecionam **Citrix Viewer**.

> A otimização do Microsoft Teams funciona por padrão com o aplicativo Citrix Workspace 2012 e posterior e macOS 10.15.

Se você quiser desabilitar a otimização do Microsoft Teams, execute este comando em um terminal e reinicie o aplicativo Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

Versão mínima - Versão mais recente do aplicativo Citrix Workspace para Chrome OS executando a versão mais recente do Chrome OS

Hardware:

- Processadores com desempenho igual ou superior ao Intel i3, quad core 2.4 GHz.

Recursos suportados:

- Áudio
- Vídeo
- Otimização de compartilhamento de tela (entrada e saída) - desabilitada por padrão. Consulte estas configurações para obter instruções sobre como ativá-la.

Escalabilidade de Servidor Único

Esta seção fornece recomendações e orientações para estimar quantos usuários ou máquinas virtuais (VMs) podem ser suportados em um único host físico. Isso é comumente referido como

Escalabilidade de Servidor Único (SSS) do Citrix Virtual Apps and Desktops. No contexto do Citrix Virtual Apps (CVA) ou virtualização de sessão, também é comumente conhecido como densidade de usuário. A ideia é descobrir quantos usuários ou VMs podem ser executados em uma única peça de hardware executando um hypervisor principal.

> **Nota:**

> Esta seção inclui orientações para estimar o SSS. Observe que as orientações são de alto nível e podem não ser necessariamente específicas para sua situação ou ambiente exclusivo. A única maneira de realmente entender o SSS do Citrix Virtual Apps and Desktops é usar uma ferramenta de escalabilidade ou teste de carga, como o Login VSI. A Citrix recomenda usar estas orientações e estas regras simples apenas para estimar rapidamente o SSS. No entanto, a Citrix recomenda usar o Login VSI ou a ferramenta de teste de carga de sua escolha para validar os resultados, especialmente antes de comprar hardware ou tomar qualquer decisão financeira.

Hardware (sistema em teste)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 @ 2,60 GHz (Turbo máximo 3,70 GHz), 12 núcleos por soquete, soquete duplo com Hyperthreading ativado
- 382 GB de RAM
- Armazenamento SSD local RAID 0 (11 discos) 6 TB

Software

Uma única máquina virtual (40 processadores lógicos) com Windows 2019 (TSVDA) executando Citrix Virtual Apps and Desktops 2106 VMware ESXi 6.7

Terminologia

- Carga de trabalho de trabalhador do conhecimento: Inclui Acrobat Reader, Freemind/Java, Visualizador de fotos, Edge e aplicativos do MS Office, como Excel, Outlook, PowerPoint e Word.
- Linha de base: Testes de escalabilidade de servidor executados com carga de trabalho de trabalhador do conhecimento (sem Microsoft Teams).
- Carga de trabalho do Microsoft Teams: Carga de trabalho típica de trabalhador do conhecimento + Microsoft Teams.

Como o Microsoft Teams é testado sob estresse

- O Microsoft Teams é otimizado com HDX. Assim, todo o processamento multimídia é descarregado para o endpoint ou cliente e não faz parte da medição.
- Todos os processos do Microsoft Teams são interrompidos ou encerrados antes do início da carga de trabalho.
- Abrir o Microsoft Teams (Inicialização a frio).
- Medir o tempo que o Microsoft Teams leva para carregar e focar na janela principal do Microsoft Teams.
- Alternar para a janela de chat usando atalhos de teclado.
- Alternar para a janela do calendário usando atalhos de teclado.
- Enviar a mensagem de chat para um usuário específico usando atalhos de teclado.
- Alternar para a janela do Microsoft Teams usando atalhos de teclado.

Resultados

- Impacto de 40% na escalabilidade com a Carga de Trabalho do Microsoft Teams (81 usuários), em comparação com a Linha de Base (137 usuários).
- Aumentar a capacidade do servidor em ~40% (em CPU) restaura o número de usuários como na carga de trabalho da Linha de Base.
- 20% de memória extra necessária com a Carga de Trabalho do Microsoft Teams, em comparação com a Linha de Base.
- Aumentar o tamanho do armazenamento por usuário em 512-1024 MB.
- Aumento de ~50% na gravação de IOPS, aumento de ~100% na leitura de IOPS. O Microsoft Teams pode ter um impacto significativo em ambientes com armazenamento mais lento.

Matriz de recursos e suporte de versão

RECURSO	MICROSOFT TEAMS (VERSÃO MÍNIMA)	VDA (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA WINDOWS CR (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA CHROME OS
Áudio/ Vídeo (P2P e conferência)	versão atual menos 90 dias	1906	1907	2009	2004	2105.5
Compartilhamento de tela	Versão atual menos 90 dias	1906	1907	2012	2006	2105.5
i. Borda vermelha do indicador de tela	Versão atual menos 90 dias	1906	2002	2012	2006	Não
ii. Limitar a captura ao Desktop Viewer	Versão atual menos 90 dias	1906	2009.5	2012	2006	Não
iii. Vários monitores	Versão atual menos 90 dias	1912 CU6+	2106 (1)	2106	2106	Não
DTMF	Versão atual menos 90 dias	N/A	2102	2101	2101	2111.1

RECURSO	MICROSOFT TEAMS (VERSÃO MÍNIMA)	VDA (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA WINDOWS CR (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA CHROME OS
Suporte a Servidor Proxy	Versão atual menos 90 dias	N/A	2012 (2)	2104 (3)	2101 (3)	2305
Compartilhamento de apps	Versão atual menos 90 dias	2109	2109.1	2203.1	2209	Não
Legendas ao Vivo	Versão atual menos 90 dias	N/A (4)	2109.1	2109	2109	2303
e911 Dinâmico	Versão atual menos 90 dias	N/A	2112.1	2112	2112	2112
Conceder Controle	Versão atual menos 90 dias	N/A	2112.1	2203.1	Não	Não
Solicitar Controle	Versão atual menos 90 dias	N/A	2112.1	2203.1	2203	2303
MultiWindow	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303

RECURSO	MICROSOFT TEAMS (VERSÃO MÍNIMA)	VDA (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA WINDOWS CR (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA MAC (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA LINUX (VERSÃO MÍNIMA)	CITRIX WORKSPACE APP PARA CHROME OS
Transcrições de Reunião	Versão atual menos 90 dias	2112.1, 1912 CU6+	2112	2203.1	2203	2303
Desfoque de Plano de Fundo	Versão atual menos 90 dias	2112, 1912 CU6+	2207	2301	2212	2303

1. Visualizador de CD somente em modo de tela cheia. SHIFT+F2 não é suportado.
2. Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também são suportados.
3. Somente anônimo.
4. Se o VDA for 2112 ou superior, as Legendas ao Vivo só funcionarão se a versão do aplicativo Citrix Workspace for 2203.1 para MAC e 2203 Linux ou 2112 para Windows. Isso ocorre porque as Legendas ao Vivo se comportam de forma diferente se o Microsoft Teams estiver no modo de interface de usuário de Janela Única ou no modo MultiJanela.
5. O MultiJanela foi introduzido no VDA 2112, mas foi retroportado para a versão VDA 1912 LTSR CU6.

> **Nota:**

> Todos os recursos listados em **Citrix Workspace app para Windows 1912 CU6 (ou posterior)** são aplicáveis ao Citrix Workspace app para Windows 2203.1 LTSR CU1.

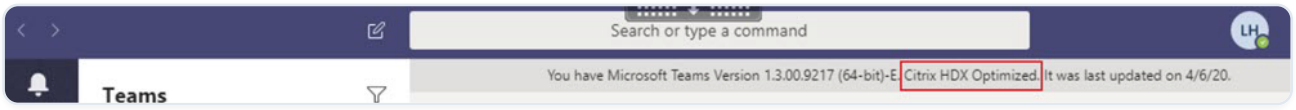
Habilitar otimização do Microsoft Teams

Para habilitar a otimização para o Microsoft Teams, use a política do Studio descrita na política Redirecionamento do Microsoft Teams. Esta política está **ATIVADA** por padrão. Além de esta

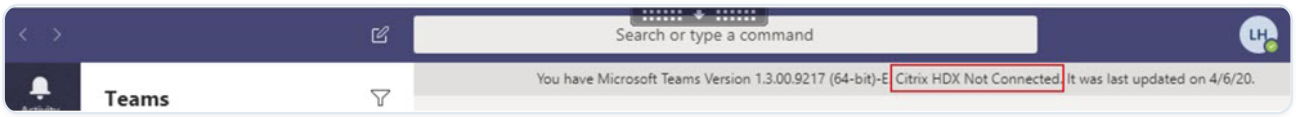
política estar habilitada, o HDX verifica se a versão do aplicativo Citrix Workspace é pelo menos a versão mínima exigida. Se você habilitou a política e a versão do aplicativo Citrix Workspace é suportada, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** é definido como **1** automaticamente no VDA. O Microsoft Teams lê a chave para carregar no modo VDI.

> **Nota:**
>
> Se você estiver usando VDAs versão 1906.2 ou posterior ou com versões de controlador mais antigas (por exemplo, versão 7.15) que não têm a política disponível no Studio, seu VDA ainda pode ser otimizado. A otimização HDX para Microsoft Teams é habilitada por padrão no VDA.

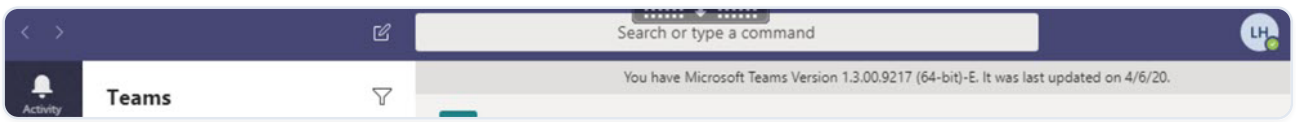
> Se você clicar em **Sobre > Versão**, a legenda **Citrix HDX Optimized** será exibida:



Se você vir **Citrix HDX Not Connected**, a API Citrix será carregada no Microsoft Teams. Carregar a API é o primeiro passo para o redirecionamento. Mas há um erro nas partes posteriores da pilha. O erro provavelmente está nos serviços VDA ou no aplicativo Citrix Workspace.



Se você não vir nenhuma legenda, o Microsoft Teams falhou ao carregar a API Citrix. Saia do Microsoft Teams clicando com o botão direito do mouse no ícone da área de notificação e reiniciando. Certifique-se de que a política do Studio não esteja definida como **Proibido** e que a versão do aplicativo Citrix Workspace seja compatível.



> **Importante: reconexões de sessão**

- Pode ser necessário reiniciar o Microsoft Teams para obter uma sessão otimizada por HDX quando sua conectividade mudar. Por exemplo, se você estiver migrando de um endpoint não compatível (aplicativo Workspace para iOS, Android ou versões antigas de

Windows/Linux/Mac) para um compatível (aplicativo Workspace para Windows/Linux/Mac/ChromeOS/HTML5), ou vice-versa.

- Uma reinicialização do Microsoft Teams também é necessária se você instalou o aplicativo usando o instalador .exe do Microsoft Teams no VDA. O instalador .exe é recomendado para implantações VDI persistentes. Nesses casos, o Microsoft Teams pode ser atualizado automaticamente enquanto a sessão HDX está no estado desconectado. Assim, os usuários que se reconectam a uma sessão HDX descobrem que o Microsoft Teams não está sendo executado de forma otimizada.
- Ao migrar de uma sessão local para uma sessão HDX, você deve reiniciar o Microsoft Teams para otimizar com HDX. Esta ação é necessária em um cenário de Acesso Remoto a PC.

Requisitos de rede

O Microsoft Teams depende de servidores Media Processor no Microsoft 365 para reuniões ou chamadas multipartidárias. Além disso, o Microsoft Teams depende dos Microsoft 365 Transport Relays para estes cenários:

- Dois pares em uma chamada ponto a ponto não têm conectividade direta
- Um participante não tem conectividade direta com o processador de mídia.

Então, a integridade da rede entre o par e a nuvem do Microsoft 365 determina o desempenho da chamada. Para diretrizes detalhadas sobre planejamento de rede, consulte Princípios de conectividade de rede do Microsoft 365.

Recomendamos avaliar seu ambiente para identificar quaisquer riscos e requisitos que possam influenciar sua implantação geral de voz e vídeo na nuvem. Use a Ferramenta de Avaliação de Rede do Skype for Business para testar se sua rede está pronta para o Microsoft Teams. Para obter informações de suporte, consulte Suporte.

Resumo das principais recomendações de rede para tráfego de Protocolo de Tempo Real (RTP)

- Conecte-se à rede do Microsoft 365 o mais diretamente possível a partir do escritório da filial.
- Planeje e forneça largura de banda suficiente no escritório da filial.
- Verifique a conectividade e a qualidade da rede em cada escritório da filial.

- Se você precisar usar qualquer um dos seguintes no escritório da filial, certifique-se de que o tráfego RTP/UDP (tratado por HdxRtcEngine.exe no aplicativo Citrix Workspace) esteja.
  - Ignorar servidores proxy
  - Interceptação SSL de rede
  - Dispositivos de inspeção profunda de pacotes
  - Hairpins de VPN (use tunelamento dividido, se possível)

Importante: Configuração de tunelamento dividido de VPN

O tráfego de HdxRtcEngine.exe deve ser desviado do túnel VPN e permitido usar a conexão de Internet local do usuário para se conectar diretamente ao serviço. A maneira como isso é realizado varia dependendo do produto VPN e da plataforma da máquina utilizada, mas a maioria das soluções VPN permitirá alguma configuração simples de política para aplicar essa lógica. Para obter mais informações sobre a orientação de tunelamento dividido específica da plataforma VPN, consulte este artigo da Microsoft.

O mecanismo de mídia WebRTC no aplicativo Workspace (HdxRtcEngine.exe) usa o Protocolo de Transporte Seguro em Tempo Real (SRTP) para fluxos multimídia que são descarregados para o cliente. O SRTP fornece confidencialidade e autenticação ao RTP. Para este recurso, chaves simétricas (negociadas com DTLS) são usadas para criptografar mídia e mensagens de controle usando a cifra de criptografia AES.

As seguintes métricas são recomendadas para uma experiência de usuário positiva:

MÉTRICA	PONTO DE EXTREMIDADE PARA MICROSOFT 365
Latência (sentido único)	< 50 ms
Latência (RTT)	< 100 ms
Perda de Pacotes	<1% durante qualquer intervalo de 15s
Jitter de interchegada de pacotes	<30ms durante qualquer intervalo de 15s

Para obter mais informações, consulte Prepare a rede da sua organização para o Microsoft Teams.

Para requisitos de largura de banda, a otimização para Microsoft Teams pode usar uma ampla variedade de codecs para áudio (OPUS/G.722/PCM G711) e vídeo (H264).

Os pares negociam esses codecs durante o processo de estabelecimento da chamada usando o Protocolo de Descrição de Sessão (SDP) Oferta/Resposta. As recomendações mínimas da Citrix por usuário são:

TIPO	LARGURA DE BANDA	CODEC
Áudio (em cada sentido)	Cerca de 90 kbps	G.722
Áudio (em cada sentido)	Cerca de 60 kbps	Opus*
Vídeo (em cada sentido)	Aproximadamente 700 kbps	H264 360p a 30 quadros por segundo 16:9
Compartilhamento de tela	Aproximadamente 300 kbps	H264 1080p a 15 quadros por segundo

Opus e H264 são os codecs preferenciais para chamadas ponto a ponto e de conferência.

> **Importante:**

> Sobre desempenho, a codificação é mais cara que a decodificação para uso da CPU na máquina cliente. Você pode codificar a resolução máxima de codificação no aplicativo Citrix Workspace para Linux e Windows. Consulte Estimador de desempenho do codificador e Otimização para Microsoft Teams.

Servidores proxy

Dependendo da localização do proxy, considere o seguinte:

- Configuração de proxy no VDA:

  Se você configurar um servidor proxy explícito no VDA e rotear as conexões para localhost através de um proxy, o redirecionamento falhará. Para configurar o proxy corretamente, você deve selecionar a configuração **Ignorar servidores proxy para endereços locais** em **Opções da Internet > Conexões > Configurações de LAN > Servidores Proxy** e ignorar `127.0.0.1:9002`.

Se você usar um arquivo PAC, seu script de configuração de proxy do VDA do arquivo PAC deve retornar **DIRECT** para `wss://127.0.0.1:9002`. Caso contrário, a otimização falhará. Para garantir que o script retorne **DIRECT**, use `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configuração de proxy no aplicativo Citrix Workspace:

  Se a filial estiver configurada para acessar a internet através de um proxy, estas versões suportam servidores proxy:

  - Aplicativo Citrix Workspace para Windows versão 2012 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também são suportados)
  - Aplicativo Citrix Workspace para Windows versão 1912 CU5 (Negotiate/Kerberos, NTLM, Basic e Digest. Arquivos `Pac` também são suportados)
  - Aplicativo Citrix Workspace para Linux versão 2101 (autenticação anônima)
  - Aplicativo Citrix Workspace para Mac versão 2104 (autenticação anônima)

Dispositivos cliente com versões anteriores do aplicativo Citrix Workspace não conseguem ler as configurações de proxy. Esses dispositivos enviam o tráfego diretamente para os servidores TURN do Microsoft 365.

Importante:

- Verifique se o dispositivo cliente pode se conectar ao servidor DNS para fazer resoluções DNS. Um dispositivo cliente deve ser capaz de resolver os seguintes FQDNs do servidor de retransmissão do Microsoft Teams:
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

> Se as solicitações DNS não forem bem-sucedidas, as chamadas P2P com usuários externos e o estabelecimento de mídia de chamadas de conferência falharão.

> - A localização do servidor de conferência é selecionada com base na localização da área de trabalho virtual do primeiro participante (e não do cliente).

Estabelecimento de chamadas e caminhos de fluxo de mídia

Quando possível, o mecanismo de mídia HDX WebRTC no aplicativo Citrix Workspace (HdxRtcEngine.exe) tenta estabelecer uma conexão direta de rede Secure Real-time Transport Protocol (SRTP) sobre User Datagram Protocol (UDP) em uma chamada ponto a ponto. Se as portas UDP altas estiverem bloqueadas, o mecanismo de mídia retorna para TCP/TLS 443.

O mecanismo de mídia HDX oferece suporte a ICE, Session Traversal Utilities for NAT (STUN) e Traversal Using Relays around NAT (TURN) para descoberta de candidatos e estabelecimento de conexão. Esse suporte significa que o endpoint deve ser capaz de realizar resoluções DNS.

Considere um cenário em que não há um caminho direto entre os dois pares ou entre um par e um servidor de conferência e você está participando de uma chamada ou reunião multipartidária. O HdxRtcEngine.exe usa um servidor de retransmissão de transporte do Microsoft Teams no Microsoft 365 para alcançar o outro par ou o processador de mídia, onde as reuniões são hospedadas. Sua máquina cliente deve ter acesso a três intervalos de endereços IP de sub-rede do Microsoft 365 e quatro portas UDP (ou TCP/TLS 443 como fallback se o UDP estiver bloqueado). Para obter mais informações, consulte o diagrama de arquitetura em Configuração de chamada e URLs e intervalos de endereços IP do Office 365 ID 11.

ID	CATEGORIA	ENDEREÇOS	PORTAS DE DESTINO
11	Otimização necessária	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (alternativa)

Esses intervalos incluem tanto os Transport Relays quanto os processadores de mídia, com um Azure Load Balancer como front-end. Os Transport Relays do Microsoft Teams fornecem funcionalidade STUN e TURN, mas não são endpoints ICE. Além disso, os Transport Relays do Microsoft Teams não encerram mídia, TLS ou realizam qualquer transcodificação. Eles podem

fazer a ponte de TCP (se HdxRtcEngine.exe usar TCP) para UDP ao encaminhar tráfego para outros pares ou processadores de mídia.

O mecanismo de mídia WebRTC do aplicativo Workspace entra em contato com o Transport Relay do Microsoft Teams mais próximo na nuvem do Microsoft 365. O mecanismo de mídia usa IP anycast e as portas UDP 3478–3481 (portas UDP diferentes por carga de trabalho, embora a multiplexação possa ocorrer) ou TCP/TLS 443 para alternativas. A qualidade da chamada depende do protocolo de rede subjacente. Como o UDP é sempre recomendado em vez do TCP, aconselhamos que você projete suas redes para acomodar o tráfego UDP no escritório remoto.

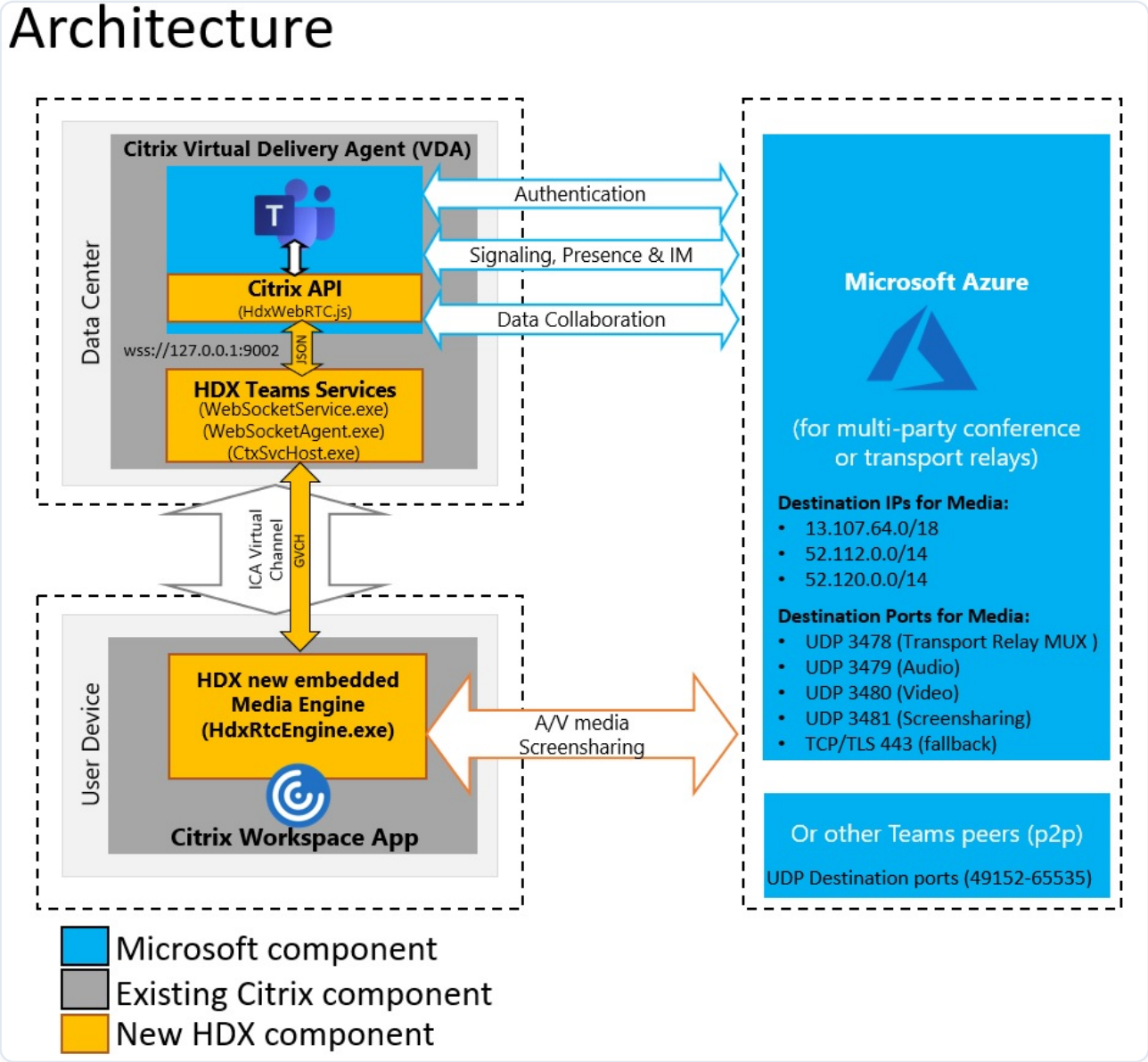
Se o Microsoft Teams for carregado no modo otimizado e HdxRtcEngine.exe estiver em execução no endpoint, falhas de ICE podem causar uma falha na configuração da chamada ou áudio/vídeo apenas unidirecional. Quando uma chamada não pode ser concluída ou os fluxos de mídia não são full duplex, verifique primeiro o **rastreamento do Wireshark** no endpoint. Para obter mais informações sobre o processo de coleta de candidatos ICE, consulte "Coleta de logs" na seção Suporte.

> **Nota:**
>
> Se os endpoints não tiverem acesso à internet, os usuários ainda poderão fazer uma chamada ponto a ponto se ambos estiverem na mesma LAN. As reuniões falham. Nesse caso, há um tempo limite de 30 segundos antes que a configuração da chamada comece.

Configuração da chamada

Use este diagrama de arquitetura como referência visual para a sequência do fluxo de chamadas. As etapas correspondentes são indicadas no diagrama.

Arquitetura



1. Iniciar o Microsoft Teams.
2. O Microsoft Teams autentica-se no O365. As políticas de locatário são enviadas para o cliente do Microsoft Teams, e as informações relevantes do canal de sinalização e TURN são retransmitidas para o aplicativo.
3. O Microsoft Teams detecta que está sendo executado em um VDA e faz chamadas de API para a API JavaScript da Citrix.
4. O JavaScript da Citrix no Microsoft Teams abre uma conexão WebSocket segura para o WebSocketService.exe em execução no VDA, que gera o WebSocketAgent.exe dentro da sessão do usuário.
5. O WebSocketAgent.exe instancia um canal virtual genérico chamando o Serviço de Redirecionamento do Microsoft Teams HDX da Citrix (CtxSvcHost.exe).

6. O wfica32.exe (mecanismo HDX) do aplicativo Citrix Workspace gera um novo processo chamado HdxRtcEngine.exe, que é o novo mecanismo WebRTC usado para otimização do Microsoft Teams.
7. O mecanismo de mídia da Citrix e o Teams.exe têm um caminho de canal virtual bidirecional e podem começar a processar solicitações multimídia.

   -----Chamadas do usuário------

8. **Par A** clica no botão **chamar**. O Teams.exe se comunica com os serviços do Microsoft Teams no Microsoft 365, estabelecendo um caminho de sinalização de ponta a ponta com o **Par B**. O Microsoft Teams solicita ao HdxRtcEngine uma série de parâmetros de chamada suportados (codecs, resoluções e assim por diante, o que é conhecido como uma oferta de Protocolo de Descrição de Sessão (SDP)). Esses parâmetros de chamada são então retransmitidos usando o caminho de sinalização para os serviços do Microsoft Teams no Microsoft 365 e, de lá, para o outro par.
9. A oferta/resposta SDP (negociação de passagem única) ocorre através do canal de sinalização, e as verificações de conectividade ICE (travessia de NAT e Firewall usando solicitações de ligação STUN) são concluídas. Em seguida, a mídia do Protocolo de Transporte em Tempo Real Seguro (SRTP) flui diretamente entre o HdxRtcEngine e o outro par (ou servidores de conferência do Microsoft 365 se for uma reunião).

Sistema Telefônico da Microsoft

O Phone System é a tecnologia da Microsoft que permite o controle de chamadas e PBX na nuvem do Microsoft 365 com o Microsoft Teams. A otimização para o Microsoft Teams oferece suporte ao Phone System, usando Planos de Chamada do Microsoft 365 ou Roteamento Direto. Com o Roteamento Direto, você conecta seu próprio controlador de borda de sessão compatível diretamente ao Microsoft Phone System sem nenhum software local adicional. Filas de chamadas, transferência, encaminhamento, espera, mudo e retomada de uma chamada são suportados.

DTMF

O recurso de multifrequência de tom duplo (DTMF) é suportado com estas versões do aplicativo Citrix Workspace (e posteriores):

- Aplicativo Citrix Workspace para Windows versão 2102
- Aplicativo Citrix Workspace para Windows LTSR 1912 CU5 (somente SO Windows 10)
- Aplicativo Citrix Workspace para Linux versão 2101
- Aplicativo Citrix Workspace para Mac versão 2101

- Aplicativo Citrix Workspace para Chrome OS versão 2111.1

Suporte para e911 dinâmico

A partir da versão 2112, o aplicativo Citrix Workspace oferece suporte a chamadas de emergência dinâmicas. Quando usado em Planos de Chamada da Microsoft, Operator Connect e Roteamento Direto, ele permite que você faça o seguinte:

- Configurar e rotear chamadas de emergência.
- Notificar o pessoal de segurança.

A notificação é fornecida com base na localização atual do aplicativo Citrix Workspace que é executado no endpoint, em vez do cliente Microsoft Teams que é executado no VDA.

A lei de Ray Baum exige que a localização despachável do chamador do 911 seja transmitida ao Ponto de Atendimento de Segurança Pública (PSAP) apropriado. A otimização do Microsoft Teams com HDX está em conformidade com a lei de Ray Baum quando usada com as seguintes versões do aplicativo Citrix Workspace:

- Aplicativo Citrix Workspace para Windows versão 2112.1 e posterior
- Aplicativo Citrix Workspace para Linux versão 2112 e posterior
- Aplicativo Citrix Workspace para Mac versão 2112 e posterior
- Aplicativo Citrix Workspace para Chrome OS versão 2112 e posterior

Para habilitar chamadas de emergência dinâmicas, o administrador deve usar o Centro de Administração do Microsoft Teams e configurar o seguinte para criar um mapa de rede ou de localização de emergência:

- Configurações de rede
- Serviço de Informações de Localização (LIS)

Para obter mais informações sobre chamadas de emergência dinâmicas, consulte a documentação da Microsoft.

As informações de localização despacháveis que o aplicativo Citrix Workspace retransmite para o Microsoft Teams são:

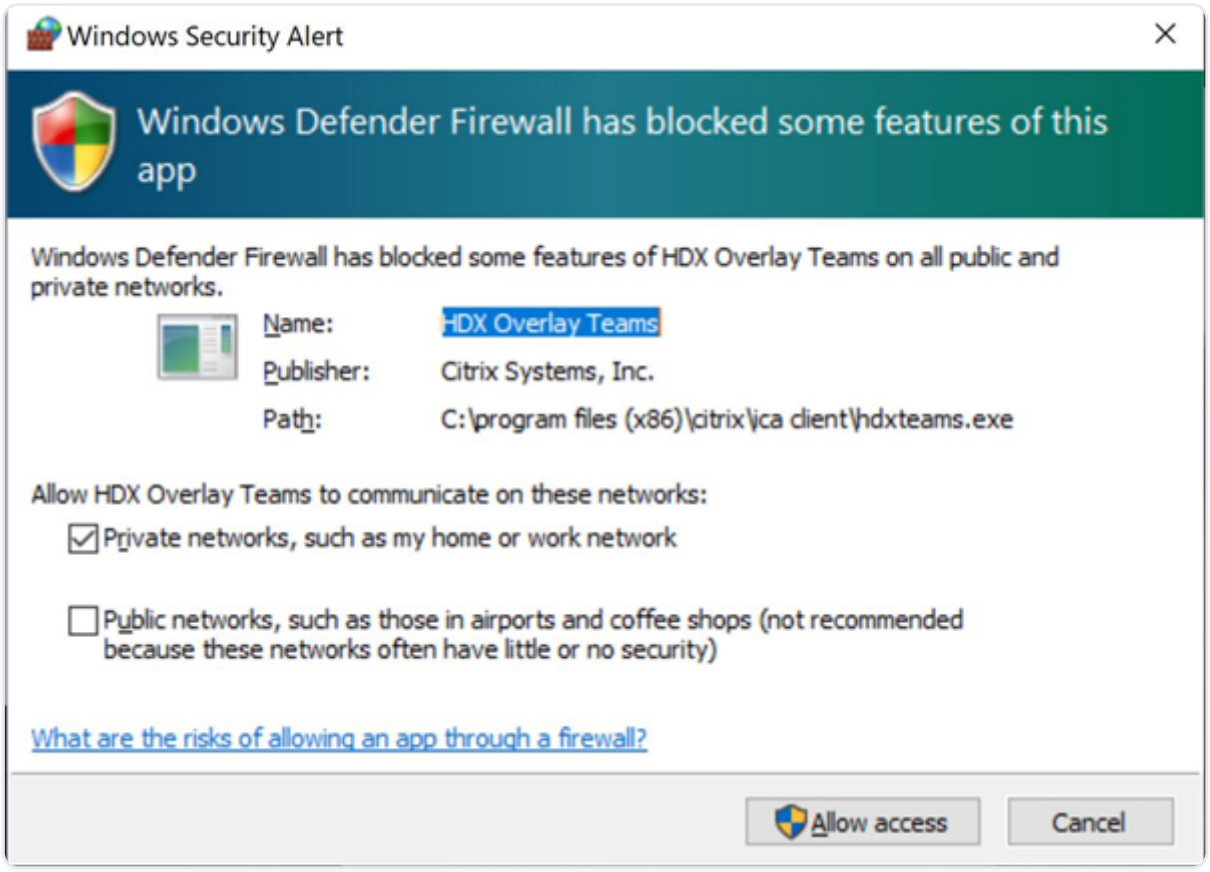
- ID do Chassi / ID da Porta usando o Protocolo de Descoberta da Camada de Link (LLDP) para conexões Ethernet/Switch. Ethernet/Switch (LLDP) é suportado em:
  - Versões do Windows 8.1 e 10

    - macOS, que requer software de habilitação LLDP. Para baixar o software de habilitação LLDP, vá para `www.microsoft.com` e procure por software de habilitação LLDP.
    - Linux, que requer que a biblioteca LLDP seja incluída na distribuição do sistema operacional (SO) do Thin Client.

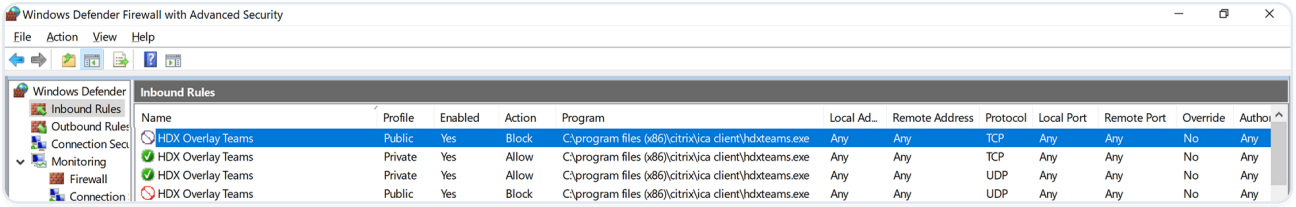
- BBSID WLAN e {IPv4-IPv6; Sub-rede; Endereço MAC} do endpoint onde o aplicativo Citrix Workspace está instalado.
    - Locais baseados em sub-rede e WiFi são suportados no aplicativo Workspace para Windows, Linux e Mac.
- Latitude e Longitude, se a permissão do usuário for concedida no nível do SO onde o aplicativo Citrix Workspace está instalado.
    - Suportado em todas as plataformas do aplicativo Workspace. No entanto, para o aplicativo Citrix Workspace para Linux, você deve incluir a biblioteca `libgps` na distribuição do SO do Thin Client (sudo apt-get install libgps23 gpsd lldpd).

Considerações sobre firewall

Quando os usuários iniciam uma chamada otimizada usando o cliente Microsoft Teams pela primeira vez, eles podem notar um aviso nas configurações do **firewall do Windows**. O aviso pede aos usuários que permitam a comunicação para HdxTeams.exe ou HdxRtcEngine.exe (HDX Overlay Microsoft Teams).



As quatro entradas a seguir são adicionadas em **Regras de Entrada** no console **Windows Defender Firewall > Segurança Avançada**. Você pode aplicar regras mais restritivas se desejar.



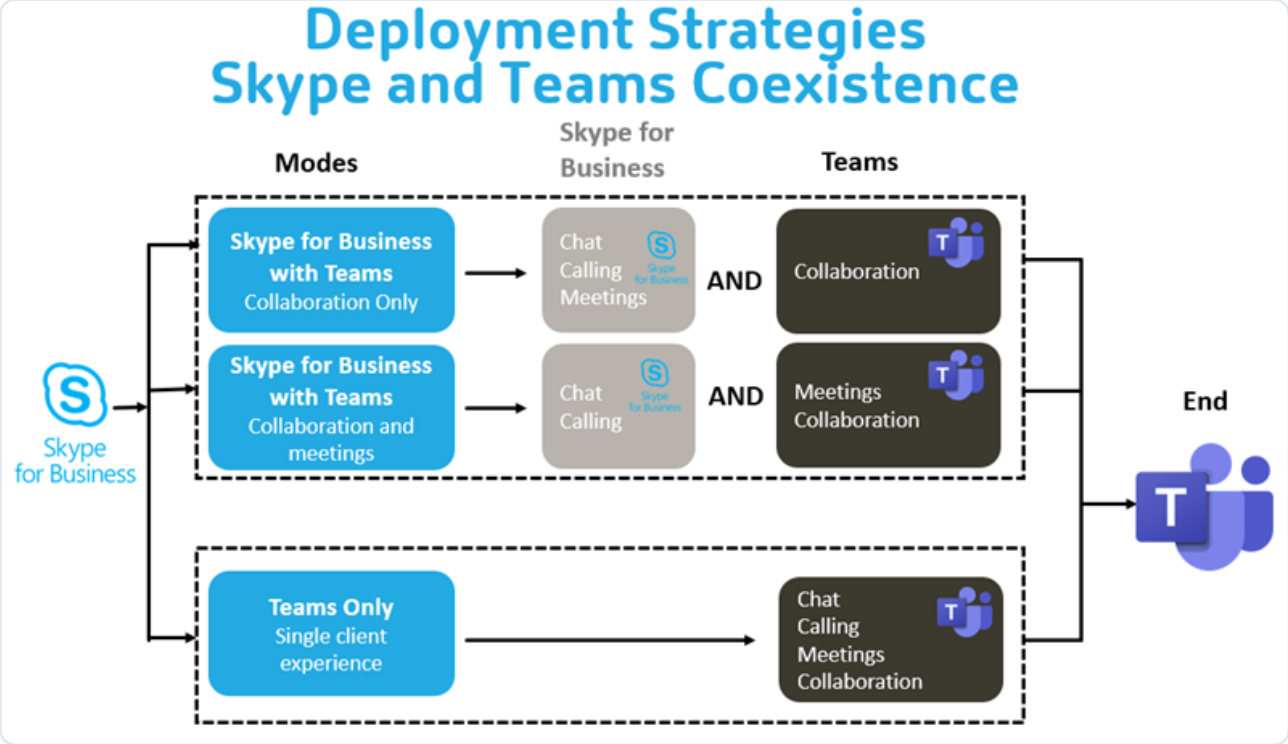
Coexistência do Microsoft Teams e do Skype for Business

Você pode implantar o Microsoft Teams e o Skype for Business lado a lado como duas soluções separadas com recursos sobrepostos. Para obter mais informações, consulte Entender a coexistência e interoperabilidade do Microsoft Teams e do Skype for Business.

O Citrix RealTime Optimization Pack e a otimização HDX para mecanismos multimídia do Microsoft Teams, então, respeitam a configuração definida em seu ambiente. Os exemplos incluem modos de ilha e Skype for Business com colaboração do Microsoft Teams. Além disso, Skype for Business com colaboração e reuniões do Microsoft Teams.

O acesso a periféricos pode ser concedido a apenas um aplicativo por vez. Por exemplo, o acesso à webcam pelo RealTime Media Engine durante uma chamada bloqueia o dispositivo de imagem

durante uma chamada. Quando o dispositivo é liberado, ele fica disponível para o Microsoft Teams.



Citrix SD-WAN™: conectividade de rede otimizada para o Microsoft Teams

A qualidade ideal de áudio e vídeo requer uma conexão de rede com a nuvem do Microsoft 365 que tenha baixa latência, baixo jitter e baixa perda de pacotes. O backhauling do tráfego RTP de áudio e vídeo do Microsoft Teams de usuários do Citrix Workspace app em filiais para um data center antes de ir para a internet pode adicionar latência excessiva. Também pode causar congestionamento em links WAN. O Citrix SD-WAN otimiza a conectividade para o Microsoft Teams seguindo os princípios de conectividade de rede do Microsoft 365. O Citrix SD-WAN usa o endereço IP e o serviço web do Microsoft 365 baseado em REST da Microsoft e o DNS próximo. Esse uso é para identificar, categorizar e direcionar o tráfego do Microsoft Teams.

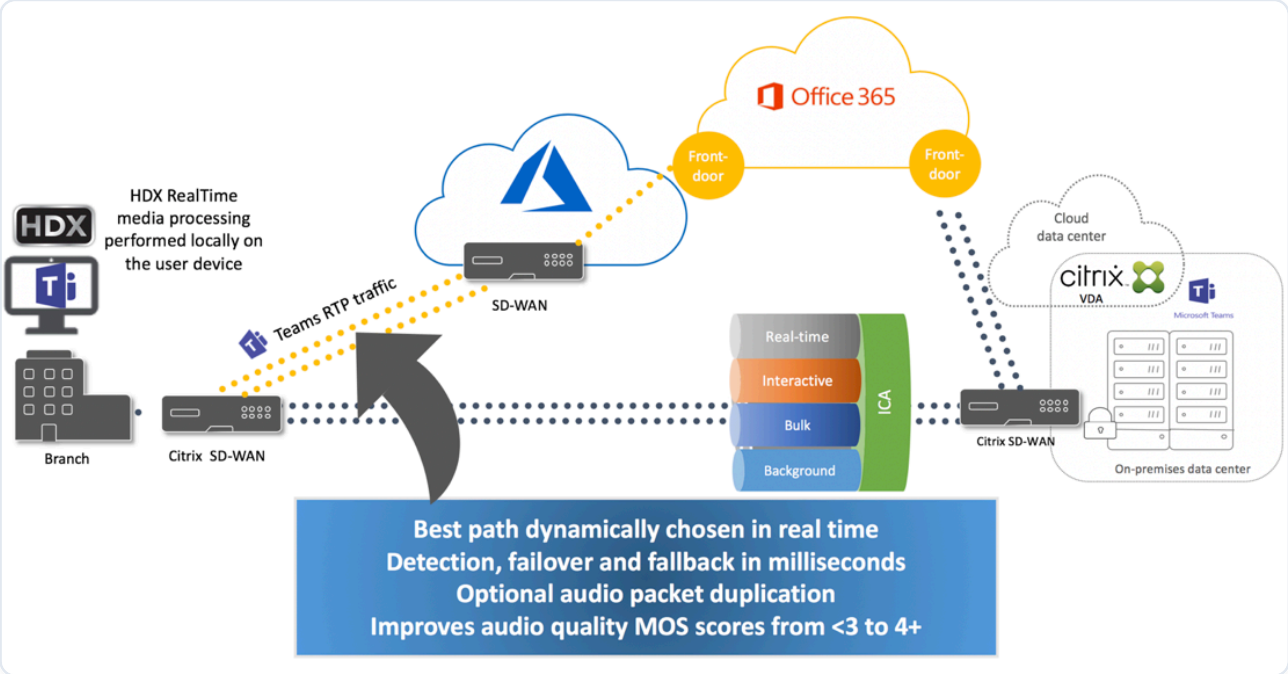
As conexões de internet banda larga empresarial em muitas áreas sofrem com perda intermitente de pacotes, períodos de jitter excessivo e interrupções.

O Citrix SD-WAN oferece duas soluções para preservar a qualidade de áudio e vídeo do Microsoft Teams quando a integridade da rede é variável ou degradada.

- Se você usa o Microsoft Azure, um appliance virtual Citrix SD-WAN (VPX) implantado na VNET do Azure oferece otimizações avançadas de conectividade. Essas otimizações incluem failover de link contínuo e corrida de pacotes de áudio.

- Os clientes do Citrix SD-WAN podem se conectar ao Microsoft 365 por meio do serviço Citrix Cloud™ Direct. Este serviço oferece entrega confiável e segura para todo o tráfego destinado à internet.

Se a qualidade da conexão de internet da filial não for uma preocupação, pode ser suficiente minimizar a latência. Direcione o tráfego do Microsoft Teams diretamente do appliance de filial do Citrix SD-WAN para o front door mais próximo do Microsoft 365 para minimizar a latência. Para obter mais informações, consulte Otimização do Citrix SD-WAN Office 365.



Reuniões e bate-papo em várias janelas

Você pode usar várias janelas de reunião ou bate-papo para o Microsoft Teams no Windows. Para obter detalhes sobre o recurso pop-out, consulte Janelas Pop-Out do Microsoft Teams para Bate-papos e Reuniões no site do Microsoft 365.

> **Nota:**
>
> Este recurso é compatível com o aplicativo Citrix Workspace para Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. Ele requer VDA 2112 ou superior e foi retroportado para 1912 CU6+ LTSR e VDA 2112.

Desfoque de fundo e efeitos de fundo

O aplicativo Citrix Workspace para Windows, Mac, Linux e ChromeOS/HTML5 oferece suporte a desfoque de fundo e efeitos de fundo na otimização do Microsoft Teams com HDX.

Você pode desfocar ou substituir o fundo por uma imagem padrão e evitar distrações inesperadas, ajudando a conversa a permanecer focada na silhueta (corpo e rosto). Você pode usar esse recurso com chamadas P2P ou de conferência.

> **Nota:**
>
> Este recurso é integrado à interface do usuário/botões do Microsoft Teams. O suporte a MultiWindow é um pré-requisito que exige uma atualização do VDA para 2112 ou posterior. Para obter mais informações, consulte Reuniões e bate-papo em várias janelas.
>
> Os controles da interface do usuário do Microsoft Teams para desfoque e efeitos de fundo exigem as seguintes versões mínimas:

- Aplicativo Citrix Workspace para Windows 2207
- Aplicativo Citrix Workspace para Mac 2301
- Aplicativo Citrix Workspace para Linux 2212
- Aplicativo Citrix Workspace para ChromeOS 2303

Limitações:

- O cliente deve estar conectado à internet ao substituir a imagem de fundo por uma imagem padrão do Microsoft Teams.
- A substituição de imagem de fundo definida pelo administrador e pelo usuário não é suportada na interface do usuário do Microsoft Teams. Imagens de fundo personalizadas podem ser configuradas usando as configurações no cliente, se a imagem também estiver armazenada no cliente.

Definindo uma imagem de fundo personalizada

As seguintes chaves de registro são necessárias apenas se você não planeja usar a interface do usuário do Microsoft Teams para controlar o recurso, ou se um administrador deseja substituir comportamentos padrão. Por exemplo, desativar o desfoque de fundo porque o endpoint não é potente o suficiente.

No Windows

Para definir uma imagem de fundo personalizada, administradores ou usuários finais devem configurar a seguinte chave de registro no cliente ou endpoint:

Local: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nome: VideoBackgroundEffect
- Tipo: DWORD
- Valor: 0 (desativado), 1 (ativado), 2 (substituição de imagem de fundo)

O valor definido como 1 desfoca o fundo. Este valor pode ser definido pelo usuário final ou pelo administrador.

O valor definido como 2 também exige que a chave **VideoBackgroundImage** esteja presente. Somente o administrador pode definir este valor. A seguinte chave é necessária apenas se você deseja substituir a imagem de fundo e não para desfoque:

- Nome: VideoBackgroundImage
- Tipo: REG_SZ
- Valor: my_image_name.jpeg

A imagem de fundo do vídeo deve estar presente no diretório `C:\Program Files (x86)\Citrix\ICA Client`.

Essa configuração de registro também pode ser usada para habilitar o desfoque de fundo ou a substituição de imagem no aplicativo Citrix Workspace 2206 sem o seletor de UI do Microsoft Teams. Em outras palavras, se seu ambiente ou VDA não suportar várias janelas, você ainda pode aplicar a solução alternativa de registro HKCU com o aplicativo Citrix Workspace 2206 ou superior para obter um resultado semelhante, embora o usuário não possa controlar a funcionalidade no meio da sessão HDX ou da chamada do Microsoft Teams.

As alterações na chave do registro só entram em vigor quando a sessão HDX se conecta.

No Mac

Local da imagem baixada pelo usuário: */Users/username/Downloads/any_image.png*

Execute os seguintes comandos para definir a imagem personalizada como a imagem padrão:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

`defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"`

No Linux

Local da imagem baixada pelo usuário: */home/username/Downloads/any_image.jpg*

Crie o arquivo */var/.config/citrix/hdx_rtc_engine/config.json* e adicione as seguintes chaves de configuração no formato JSON. Por exemplo,

```
{


"VideoBackgroundEffect":2,


"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"


}
```

No HTML5

Para HTML5, apenas o desfoque de fundo é suportado. A substituição de imagem personalizada não é suportada.

Para o desfoque de fundo, faça o seguinte:

1. navegar até o arquivo **configuration.js** na pasta **HTML5Client**.
2. Adicione o atributo **backgroundEffects** e defina o atributo como **true**. Por exemplo,

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true

    }
```

```
}
```

3. Salve as alterações.

Considerações sobre o consumo de CPU do cliente

Embora o recurso de desfoque seja econômico em termos de CPU, você pode esperar um aumento no consumo. Por exemplo, em um thin client com um chip Intel® Pentium® Silver de 4 núcleos, 1,5 GHz com TurboBoost de até 2,8 GHz, o desfoque de fundo adiciona cerca de 2% ao uso da CPU. O uso médio da CPU é inferior a 20%.

Visualização de galeria e oradores ativos no Microsoft Teams

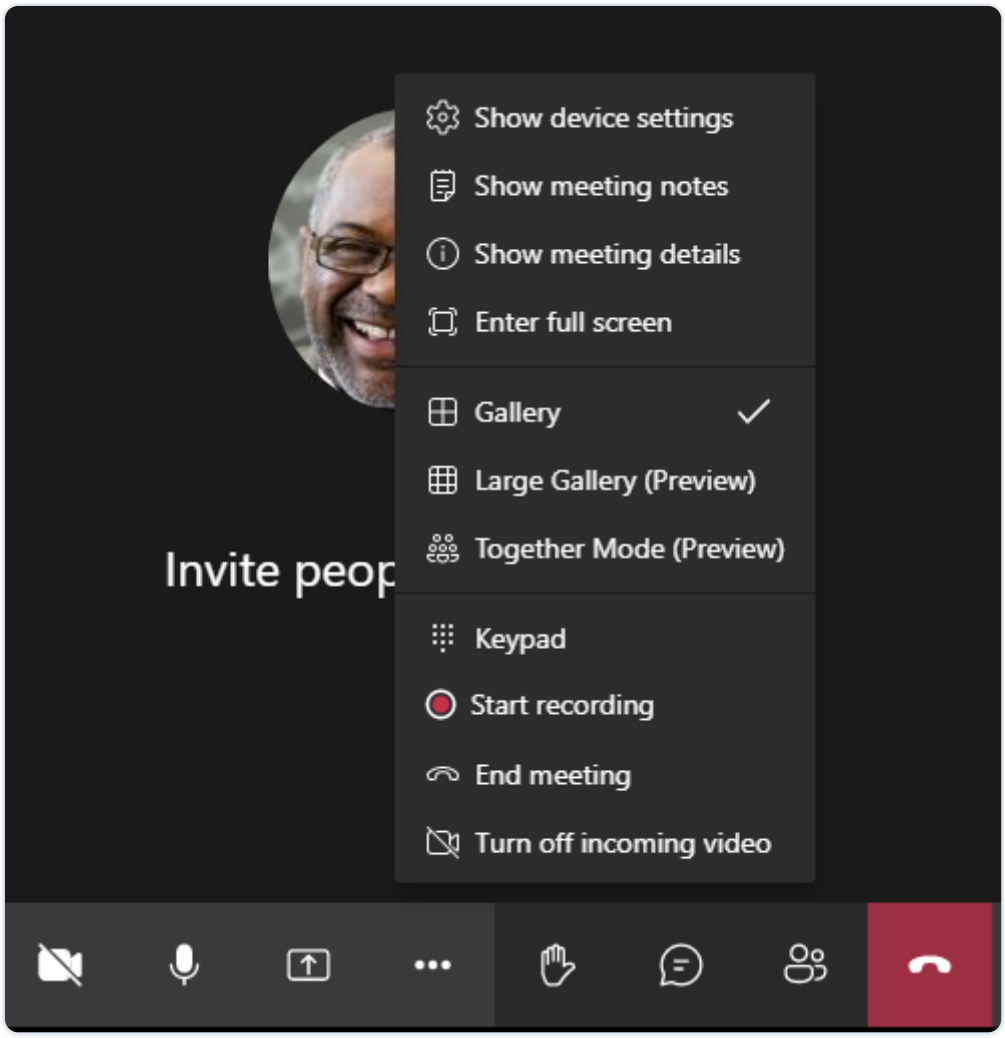
O Microsoft Teams oferece suporte aos layouts **Galeria**, **Galeria grande** e **Modo Juntos**.

O Microsoft Teams exibe uma grade 2x2 com fluxos de vídeo de quatro participantes (conhecida como **Galeria**). Nesse caso, o Microsoft Teams envia quatro fluxos de vídeo para o dispositivo cliente para decodificação. Quando mais de quatro participantes compartilham vídeo, apenas os quatro oradores mais ativos aparecem na tela.

O Microsoft Teams também oferece a visualização de galeria grande com uma grade de até 7x7. Como resultado, o servidor de conferência do Microsoft Teams compõe um único feed de vídeo e o envia para o dispositivo cliente para decodificação, resultando em menor consumo de CPU. Esse feed único, estilo matriz, também pode incluir o vídeo de auto-visualização dos usuários.

Por fim, o Microsoft Teams oferece suporte ao **Modo Juntos**, que faz parte da nova experiência de reunião. Usando a tecnologia de segmentação de IA para posicionar digitalmente os participantes em um plano de fundo compartilhado, o Microsoft Teams coloca todos os participantes no mesmo auditório.

O usuário pode controlar esses modos durante uma chamada de conferência selecionando os layouts **Galeria**, **Galeria grande** ou **Modo Juntos** no menu de reticências.



Suporte para restrições de proporção de vídeo (CWA para Windows 2102, CWA para Linux 2106, CWA para MAC 2106 e posterior):

- A opção **Preencher para enquadrar** está disponível na Visualização de Galeria/Galeria Grande. Esta opção corta o tamanho do vídeo para ajustá-lo na subjanela. **Ajustar ao quadro**, por outro lado, exibe barras pretas (letterbox) nas laterais do vídeo para que não haja corte.

A tabela a seguir fornece uma comparação dos layouts de Galeria e Galeria Grande:

	VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO)	VISUALIZAÇÃO DE GALERIA AMPLA
Layout / Grade	Exibe uma grade 2x2 com fluxos de vídeo de quatro participantes. Apenas os quatro oradores mais ativos aparecem na tela e outros participantes não aparecem na grade.	Exibe uma grade 7x7 com fluxos de vídeo de 49 participantes.

	VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO)	VISUALIZAÇÃO DE GALERIA AMPLA
Técnica de mixagem	Um roteador de mídia encaminha fluxos individuais de cada participante para cada usuário.	Um servidor de conferência central mixa e transcodifica todo o áudio ou vídeo para criar um layout composto personalizado para cada participante. Essa ação introduz alguma latência adicional.
Orador ativo	O novo orador ativo substitui o orador menos ativo na grade.	Exibe todos os participantes independentemente de estarem ativos ou inativos.
Codificação no endpoint	Um ou mais fluxos de vídeo podem ser codificados no endpoint se o Simulcast estiver habilitado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.	Um ou mais fluxos de vídeo podem ser codificados no endpoint se o Simulcast estiver habilitado. Para obter mais informações sobre o suporte a Simulcast, consulte Simulcast.
Decodificação no endpoint	Cada participante recebe até quatro fluxos de mídia individuais. Isso aumenta o consumo de CPU no endpoint pelo HdxRtcEngine.exe (para decodificação/renderização).	Cada participante recebe apenas um único fluxo para áudio e vídeo. Essa configuração reduz o consumo de CPU no endpoint.
Resolução máxima	720p. Quando quatro participantes estão compartilhando vídeo, a resolução máxima é de 360p por feed de vídeo. Se menos de quatro participantes estiverem compartilhando vídeo, a resolução por feed de vídeo pode ser maior.	720p para o layout composto ou mixagem. Não há necessidade de um fluxo de vídeo de alta qualidade por participante em um layout composto. Devido a essa condição, cada remetente reduz a resolução ou a taxa de bits de upload.

	VISUALIZAÇÃO DE GALERIA 2X2 (PADRÃO)	VISUALIZAÇÃO DE GALERIA AMPLA
Problema de 'usuário lento'	O remetente modifica a qualidade de cada modalidade (áudio/vídeo/ compartilhamento de tela) para a menor qualidade de rede comum entre os participantes. Este fluxo multimídia é então encaminhado para todos os outros participantes. Como resultado, um participante com condição de rede ruim afeta a qualidade para todos os outros na chamada.	Menos suscetível ao cenário de menor qualidade de rede comum. O servidor de conferência oferece diferentes qualidades com base nas condições de rede dos participantes individuais.
Pré-visualização	Exibe você em uma pequena miniatura em tempo real.	Exibe você em miniatura e misturado com o restante dos feeds de vídeo. Como resultado, você pode se ver incluído no layout de vídeo principal com algum atraso adicional.

Compartilhamento de tela no Microsoft Teams

O Microsoft Teams depende do compartilhamento de tela baseado em vídeo (VBSS), codificando efetivamente a área de trabalho compartilhada com codecs de vídeo como H264 e criando um fluxo de alta definição. Com a otimização HDX, o compartilhamento de tela de entrada é tratado como um fluxo de vídeo.

A partir do Citrix Workspace app 2109 ou superior para Windows, Linux, Mac, e Citrix Workspace app 2303 para ChromeOS, os usuários podem compartilhar suas telas e câmera de vídeo simultaneamente.

Com versões anteriores, se você estiver no meio de uma chamada de vídeo e o outro colega começar a compartilhar a área de trabalho, o feed de vídeo original da câmera será pausado. Em vez disso, o feed de vídeo de compartilhamento de tela é exibido. O colega deve então retomar manualmente o compartilhamento da câmera.

Observação para o PowerPoint Live

Essa limitação não existe se você estiver compartilhando conteúdo do PowerPoint Live. Nesse caso, outros participantes ainda podem ver sua webcam e conteúdo e navegar para frente e para trás para revisar outros slides. Nesse cenário, os slides são renderizados no VDA. Para acessar um conjunto de slides do PowerPoint Live, clique no botão 'Share tray' e selecione um dos slides sugeridos do PowerPoint, ou clique em 'Browse' e encontre um arquivo do PowerPoint em seu computador ou no OneDrive.

O compartilhamento de tela de saída também é otimizado e descarregado para o aplicativo Citrix Workspace. Nesse caso, o mecanismo de mídia captura e transmite apenas a janela do Citrix Desktop Viewer (CDViewer.exe), com uma borda vermelha desenhada ao redor dela. Qualquer aplicativo local que se sobreponha ao Desktop Viewer não é capturado.

Nota

Defina permissões específicas no aplicativo Citrix Workspace para Mac para habilitar o compartilhamento de tela. Para obter mais informações, consulte Requisitos do sistema.

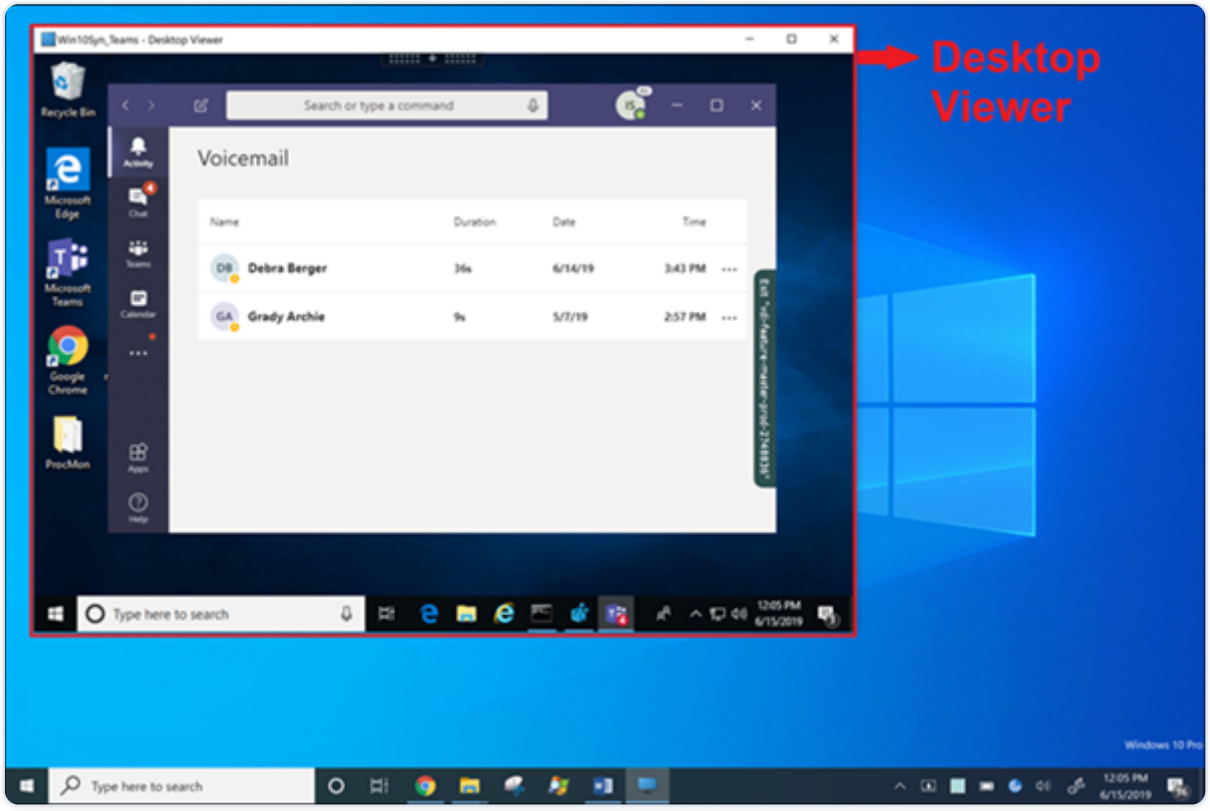
Multimonitor

Se o Desktop Viewer (CDViewer.exe) estiver em modo de tela cheia e abrangendo configurações de vários monitores, o aplicativo Citrix Workspace 2106 ou posterior (Windows/Linux/Mac) permite que o seletor de tela escolha o monitor a ser compartilhado.

Limitação conhecida:

- Se o Desktop Viewer estiver desabilitado ou se o Desktop Lock estiver sendo usado, a seleção de vários monitores não estará disponível no seletor de tela do Microsoft Teams. O Desktop Viewer pode ser desabilitado editando o modelo de arquivo `.ICA` ou `StoreFront web.config`. A tecla de atalho SHIFT+F2 não é compatível com o compartilhamento de tela em vários monitores.
- Em versões do aplicativo Workspace anteriores à 2106, apenas o monitor principal é compartilhado. Arraste o aplicativo na área de trabalho virtual para o monitor principal para que o outro participante da chamada possa vê-lo.

- O compartilhamento de tela em vários monitores pode não funcionar se você configurar o aplicativo Citrix Workspace com o recurso de layout de monitor virtual (partição lógica de um único monitor físico). Nesse caso, todos os monitores virtuais são compartilhados como uma imagem composta.
- Versões mais antigas do aplicativo Citrix Workspace para Windows (1907 até 2008) também compartilham um aplicativo local que é executado na máquina cliente. Esse compartilhamento é possível apenas se o aplicativo local estiver sobreposto ao Desktop Viewer. Esse comportamento foi removido nas versões 2009.6 ou superiores e 1912 CU5 ou superiores.
- Durante o compartilhamento de tela, se você mudar do modo janela para tela cheia, o compartilhamento de tela para. Você deve parar e compartilhar novamente para que o compartilhamento de tela funcione.



Compartilhamento de tela de aplicativo contínuo:

Se você estiver publicando o Microsoft Teams como um aplicativo autônomo e contínuo, o compartilhamento de tela capturará a área de trabalho local do seu endpoint físico. É necessária a versão mínima 1909 do aplicativo Citrix Workspace.

Compartilhamento de apps

A partir do aplicativo Citrix Workspace para Windows 2112.1 e VDA 2112, o Microsoft Teams oferece suporte ao compartilhamento de aplicativos.

A partir do aplicativo Citrix Workspace para Windows 2109, Mac 2203, Linux 2209 e VDA 2109, o Microsoft Teams oferece suporte ao compartilhamento de tela de aplicativos específicos em execução na sessão virtual. Para compartilhar um aplicativo específico:

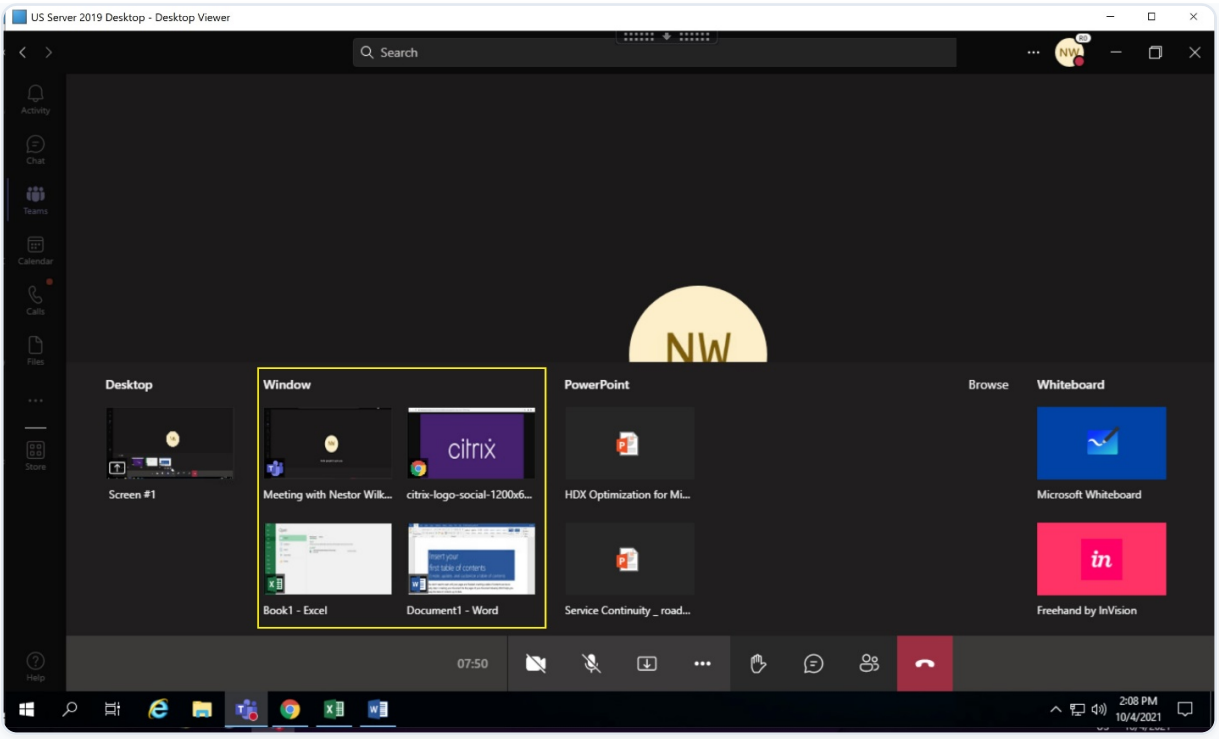
1. navegar para o aplicativo Microsoft Teams dentro da sua sessão remota.
2. Clique em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams.
3. Selecione um aplicativo para compartilhar na reunião. A borda vermelha aparece ao redor do aplicativo selecionado e os participantes da chamada podem ver o aplicativo compartilhado.

Para compartilhar um aplicativo diferente, clique em **Compartilhar conteúdo** novamente e selecione um novo aplicativo.

Se você quiser desabilitar o compartilhamento de aplicativos, crie a seguinte chave de registro no VDA em `HKLM\SOFTWARE\Citrix\Graphics`: Nome: `UseWsProvider` Tipo: `DWORD` Valor: 0

Nota:

- Quando a atualização for lançada pela Microsoft, você poderá verificar CTX253754 para a atualização da documentação e o anúncio.
- Se você minimizar um aplicativo, o Microsoft Teams exibirá a última imagem do aplicativo compartilhado. Você pode maximizar a janela para retomar o compartilhamento de tela.
- O compartilhamento de tela depende da captura da janela no lado do VDA. O conteúdo é então retransmitido a uma taxa máxima para o aplicativo Citrix Workspace. A taxa máxima é de 30 quadros por segundo. O aplicativo Citrix Workspace encaminha o conteúdo para os pares ou para o servidor de conferência.



Limitações conhecidas com o compartilhamento de tela de aplicativos específicos:

- O ponteiro do mouse não fica visível ao compartilhar a tela de um aplicativo.
- Se você minimizar um aplicativo enquanto o estiver compartilhando, apenas o ícone do aplicativo aparecerá no seletor de tela. A miniatura do aplicativo não é visualizada no seletor de tela. Você não pode compartilhar o conteúdo e a borda vermelha não aparece até que você maximize o aplicativo.
- Os aplicativos LAA mostram uma lista de aplicativos que podem ser compartilhados com aplicativos de desktop no Microsoft Teams otimizado no VDA. No entanto, ao selecionar o aplicativo na lista, o resultado pode não ser o esperado.

Compatibilidade com a proteção de aplicativos O compartilhamento de tela de um aplicativo específico é compatível com o recurso de proteção de aplicativos no Microsoft Teams otimizado para HDX. Você pode compartilhar a tela de um aplicativo específico se tiver iniciado o aplicativo ou a área de trabalho de um grupo de entrega que tenha a proteção de aplicativos ativada.

Ao clicar em **Compartilhar conteúdo** na interface do usuário do Microsoft Teams, o seletor de tela remove a opção **Desktop**. Você só pode selecionar a opção **Janela** para compartilhar qualquer aplicativo aberto.

> **Nota:**

> Ao iniciar aplicativos ou áreas de trabalho de um grupo de entrega com a proteção de aplicativos ativada, você não consegue ver o vídeo ou o compartilhamento de tela de entrada.

Conceder e solicitar controle no Microsoft Teams

Este recurso é compatível com as seguintes versões do aplicativo Citrix Workspace (não há dependência da versão do VDA ou do sistema operacional, sessão única ou multissessão):

- Aplicativo Citrix Workspace para Windows versão 2112.1 e posterior
- Aplicativo Citrix Workspace para Mac versão 2203.1 e posterior
- Aplicativo Citrix Workspace para Linux versão 2203 e posterior
- Aplicativo Citrix Workspace para ChromeOS versão 2303 e posterior

Você pode solicitar o controle durante uma chamada do Microsoft Teams quando um participante estiver compartilhando a tela. Depois de ter o controle, você pode fazer seleções, edições ou outras atividades de teclado e mouse na tela compartilhada.

Para assumir o controle quando uma tela estiver sendo compartilhada, clique no botão **Solicitar controle** na interface do usuário do Microsoft Teams. O participante da reunião que está compartilhando a tela pode permitir ou negar sua solicitação.

Enquanto você tiver o controle, poderá fazer seleções, edições e outras modificações na tela compartilhada. Para essas ações, você pode usar o teclado e o mouse. Quando terminar, clique em **Solicitar controle**.

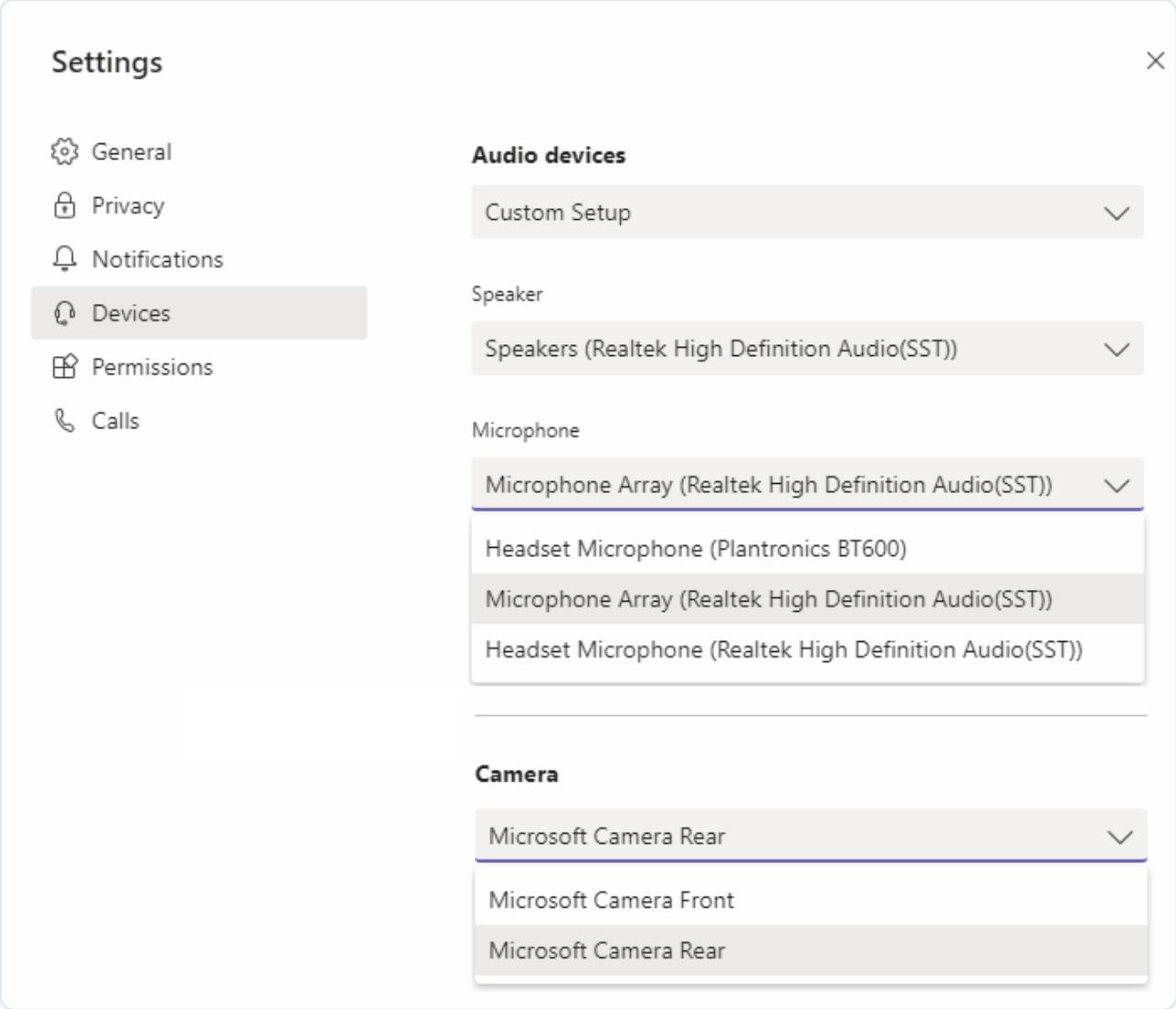
> **Limitações:**

> - Conceder e Solicitar controle não estão disponíveis se o usuário estiver compartilhando um único aplicativo (também conhecido como Compartilhamento de aplicativo). A área de trabalho ou o monitor completo deve ser compartilhado.
> - O recurso para fixar a barra de controle em um local específico não está disponível.

Periféricos no Microsoft Teams

Quando a otimização para Microsoft Teams está ativa, o aplicativo Citrix Workspace acessa os periféricos (fones de ouvido, microfones, câmeras, alto-falantes e assim por diante). Então, os

periféricos são listados corretamente na interface do usuário do Microsoft Teams (**Configurações > Dispositivos**).



O Microsoft Teams não acessa os dispositivos diretamente. Em vez disso, ele depende do mecanismo de mídia WebRTC do aplicativo Workspace para adquirir, capturar e processar a mídia. O Microsoft Teams lista os dispositivos para o usuário selecionar.

Os periféricos inseridos enquanto o Microsoft Teams está ativo não são selecionados por padrão. Você precisa selecionar manualmente os periféricos na tela **Configurações** > **Dispositivos** da interface do usuário do Microsoft Teams. Depois que o periférico é selecionado, o Microsoft Teams armazena em cache as informações dos periféricos. Como resultado, os periféricos são selecionados automaticamente quando você se reconecta a uma sessão do mesmo endpoint.

Recomendações:

- Fones de ouvido certificados para Microsoft Teams com cancelamento de eco integrado. Em configurações com periféricos extras, onde microfone e alto-falantes estão em dispositivos

separados, pode haver um eco. Um exemplo é uma webcam com microfone integrado e um monitor com alto-falantes. Ao usar alto-falantes externos, posicione-os o mais longe possível do microfone. Além disso, posicione-os longe de qualquer superfície que possa refratar o som para o microfone.

- Câmeras certificadas para Microsoft Teams, embora periféricos certificados para Skype for Business sejam compatíveis com o Microsoft Teams.
- O mecanismo de mídia do aplicativo Citrix Workspace não pode aproveitar o descarregamento da CPU com webcams que realizam codificação H.264 integrada - UVC 1.1 e 1.5.

Nota:

O aplicativo Workspace 2009.6 para Windows agora pode adquirir periféricos com formatos de áudio de 24 bits ou com frequências acima de 96 kHz.

HdxTeams.exe (no aplicativo Citrix Workspace para Windows 2009 ou anterior) suporta apenas estes formatos específicos de dispositivo de áudio (canais, profundidade de bits e taxa de amostragem):

- Dispositivos de Reprodução: até 2 canais, 16 bits, frequências de até 96.000 Hz
- Dispositivos de Gravação: até 4 canais, 16 bits, frequências de até 96.000 Hz

Mesmo que um alto-falante ou microfone não corresponda às configurações esperadas, a enumeração de dispositivos no Microsoft Teams falha e **Nenhum** é exibido em **Configurações > Dispositivos**.

Os logs do **Webrpc** em **HdxTeams.exe** mostram este tipo de informação:

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

`Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!` !

Como solução alternativa, desative o dispositivo específico ou:

1. Abra o **Painel de Controle de Som** (mmsys.cpl).
2. Selecione o dispositivo de reprodução ou gravação.
3. Vá para **Propriedades > Avançado** e altere as configurações para um modo compatível.

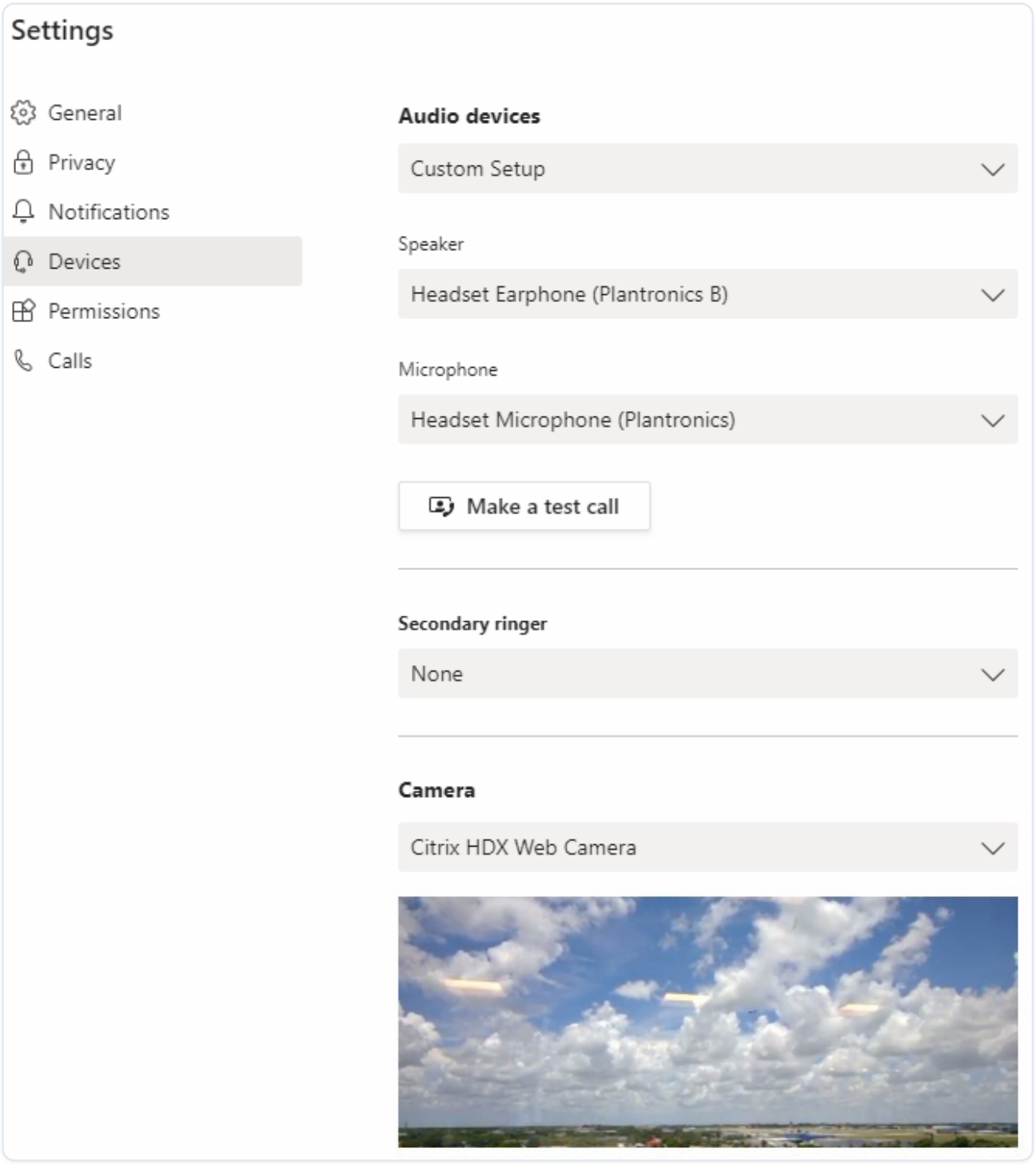
Modo de fallback

Se o Microsoft Teams falhar ao carregar no modo VDI otimizado ("Citrix HDX Not Connected" em Teams/Sobre/Versão), o VDA retorna às tecnologias HDX legadas. As tecnologias HDX legadas podem ser o redirecionamento de webcam e o redirecionamento de áudio e microfone do cliente. Se você estiver usando uma versão do aplicativo Workspace/SO de plataforma que não oferece suporte à otimização do Microsoft Teams, as chaves de registro de fallback não se aplicam. No modo de fallback, os periféricos são mapeados para o VDA. Os periféricos aparecem para o aplicativo Microsoft Teams como se estivessem conectados localmente à área de trabalho virtual.

Agora você pode controlar granularmente o mecanismo de fallback definindo as chaves de registro no VDA. Para obter informações, consulte Modo de fallback do Microsoft Teams na lista de recursos gerenciados por meio do registro.

Este recurso requer a versão 1.3.0.13565 ou posterior do Microsoft Teams.

Para determinar se você está no modo otimizado ou não otimizado ao visualizar a guia **Configurações > Dispositivos** no aplicativo Microsoft Teams, a principal diferença é o nome da câmera. Se o Microsoft Teams for carregado no modo não otimizado, as tecnologias HDX legadas serão iniciadas. O nome da webcam tem o sufixo **Citrix HDX**, conforme mostrado na imagem a seguir. Os nomes dos dispositivos de alto-falante e microfone podem ser ligeiramente diferentes (ou truncados) em comparação com o modo otimizado.



Quando tecnologias HDX legadas são usadas, o Microsoft Teams não descarrega o processamento de áudio, vídeo e compartilhamento de tela para o mecanismo de mídia WebRTC do aplicativo Citrix Workspace do endpoint. Em vez disso, as tecnologias HDX usam renderização do lado do servidor. Espere alto consumo de CPU no VDA ao ligar o vídeo. O desempenho de áudio em tempo real pode não ser ideal.

Limitações conhecidas

Limitações do Citrix

Limitações no aplicativo Citrix Workspace:

- Botões HID - Atender e encerrar chamadas não são suportados. Aumentar e diminuir o volume são suportados.
- As configurações de QoS no Centro de Administração para Microsoft Teams não se aplicam a usuários VDI.
- O recurso de complemento de proteção de aplicativo para o aplicativo Citrix Workspace impede o compartilhamento de tela de saída e bloqueia o compartilhamento de tela e vídeo de entrada.
- Os usuários não podem tirar capturas de tela do conteúdo do Microsoft Teams ao usar uma ferramenta de recorte no VDA. No entanto, se uma ferramenta de recorte for usada no lado do cliente, o conteúdo pode ser capturado.

Limitação no VDA:

- Quando você configura a configuração de DPI Alto do aplicativo Citrix Workspace para **Sim**, a janela de vídeo redirecionada aparece fora do lugar. Essa limitação ocorre quando o fator de escala de DPI do monitor é definido para qualquer valor acima de 100%.

Limitações no aplicativo Citrix Workspace e no VDA:

- Você só pode controlar o volume de uma chamada otimizada usando a barra de volume na máquina cliente — não no VDA.

Simulcast

O suporte a Simulcast está habilitado para chamadas de videoconferência otimizadas do Microsoft Teams no Windows e Mac. Para Linux, verifique com o fornecedor do seu thin client. Com o Simulcast, a qualidade e a experiência das chamadas de videoconferência em diferentes endpoints são aprimoradas, adaptando-se à resolução adequada para a melhor experiência de chamada para todos os participantes.

Com esta experiência aprimorada, cada usuário pode entregar múltiplos fluxos de vídeo em diferentes resoluções (por exemplo, 720p, 360p, e assim por diante) dependendo de vários fatores, incluindo a capacidade do endpoint, condições de rede, e assim por diante. O endpoint receptor então solicita a resolução de qualidade máxima que ele pode manipular, proporcionando assim a todos os usuários a experiência de vídeo ideal.

Nota:

Este recurso está disponível somente após o lançamento de uma atualização do Microsoft Teams. Para informações sobre o ETA, `<https://www.microsoft.com/>` acesse e pesquise pelo roteiro do Microsoft 365. Quando a atualização for lançada pela Microsoft, você pode verificar CTX253754 para a atualização da documentação e o anúncio.

Limitações do Microsoft

- A visualização de galeria 3x3 não é suportada. Dependência do Microsoft Teams – entre em contato com a Microsoft para saber quando esperar uma grade 3x3.
- A interoperabilidade com o Skype for Business é limitada a chamadas de áudio, sem modalidade de vídeo.
- A resolução máxima do fluxo de vídeo de entrada e saída é 720p. Dependência do Microsoft Teams – entre em contato com a Microsoft para saber quando esperar 1080p.
- O tom de retorno de chamada PSTN não é suportado.
- O desvio de mídia para Roteamento Direto não é suportado.
- As funções de produtor e apresentador de transmissão e evento ao vivo não são suportadas. A função de participante é suportada, mas não otimizada (renderiza no VDA em vez disso).
- A função de zoom in e zoom out no Microsoft Teams não é suportada.
- O Roteamento Baseado em Localização e o Desvio de Mídia não são suportados.
- A fusão de chamadas não é suportada (opção não exibida na interface do usuário).

Limitações do Citrix e Microsoft

- Ao compartilhar a tela, a opção **incluir áudio do sistema** não está disponível.
- Simulcast não é suportado no ChromeOS.

Próximo EOL do Microsoft Teams de Janela Única

Em January 31, 2024, a Microsoft descontinuará o suporte do Microsoft Teams para a interface de usuário de janela única ao usar a otimização do Microsoft Teams VDI e suportará apenas a experiência de múltiplas janelas. A Microsoft notificou essa descontinuação em 9/8/2023 no Centro de Administração do M365 (ID da Postagem: MC674419). Detalhes públicos sobre o recurso de

Múltiplas Janelas podem ser encontrados no artigo da Comunidade Técnica: New Meeting and Calling Experience in Microsoft Teams.

Você deve atualizar seu VDA e o aplicativo Citrix Workspace para as versões suportadas para continuar usando o Microsoft Teams no modo otimizado para vídeo e compartilhamento de tela. Se você não atualizar sua infraestrutura e endpoints para suportar múltiplas janelas, você poderá apenas estabelecer chamadas de áudio. Você não poderá usar a funcionalidade otimizada de vídeo e compartilhamento de tela.

A tabela a seguir ilustra as versões mínima, LTSR e recomendada do VDA e do aplicativo Citrix Workspace necessárias para continuar usando chamadas otimizadas no Microsoft Teams em Citrix VDI:

COMPONENTE	VERSÃO MÍNIMA	VERSÃO LTSR SUPORTADA	VERSÃO RECOMENDADA
Microsoft Teams	1.5.00.11865	Não aplicável	Mais recente
VDA	1912 CU6 LTSR, 2203 LTSR, 2112 CR	1912 CU7+, 2203 CU2+	2308 CR+
Aplicativo Citrix Workspace para Windows	2205 CR	2203 CU2+	2309 CR+
Aplicativo Citrix Workspace para Mac	2209 CR	Não aplicável	2308 CR+
Aplicativo Citrix Workspace para Linux	2209 CR	Não aplicável	2308 CR+
Aplicativo Citrix Workspace para ChromeOS ou HTML5	2303 CR	Não aplicável	2309 CR+

Anúncio de descontinuação do formato SDP (Plano B) do WebRTC

A Citrix planeja descontinuar o suporte ao formato SDP atual (Plano B) do WebRTC em futuras versões. Você deve usar o Plano Unificado no WebRTC para oferecer suporte às funcionalidades otimizadas do Microsoft Teams.

Produtos afetados

Em uma das futuras versões do Citrix Workspace Application, chamadas entre endpoints com a próxima versão do aplicativo Citrix Workspace e endpoints com o aplicativo Citrix Workspace 2108 ou versões mais antigas não serão suportadas. Essa incompatibilidade de chamada inclui clientes do aplicativo Citrix Workspace 1912 LTSR (CWA). Os seguintes clientes CWA são afetados:

- Aplicativo Citrix Workspace para Windows
- Aplicativo Citrix Workspace para Linux
- Aplicativo Citrix Workspace para Mac
- Aplicativo Citrix Workspace para Chrome

Substituição para o Plano B

Se você estiver executando uma versão do aplicativo Citrix Workspace anterior à 2109, deverá atualizar para uma versão compatível (preferencialmente a versão CR mais recente). Caso contrário, quaisquer chamadas com uma versão futura ou endpoints mais recentes falharão ao conectar. Chamadas entre versões futuras e seus parceiros de comunicação federados também podem falhar se o parceiro federado não tiver atualizado seu aplicativo Citrix Workspace.

A versão 2108 do aplicativo Citrix Workspace encerrou sua data de suporte em março de 2023 e deve ser atualizada para uma versão mais recente. Para obter mais informações, consulte Workspace App para detalhes sobre o suporte à versão do aplicativo Citrix Workspace.

Para obter mais informações sobre a descontinuação do Plano B, consulte a documentação do WebRTC.

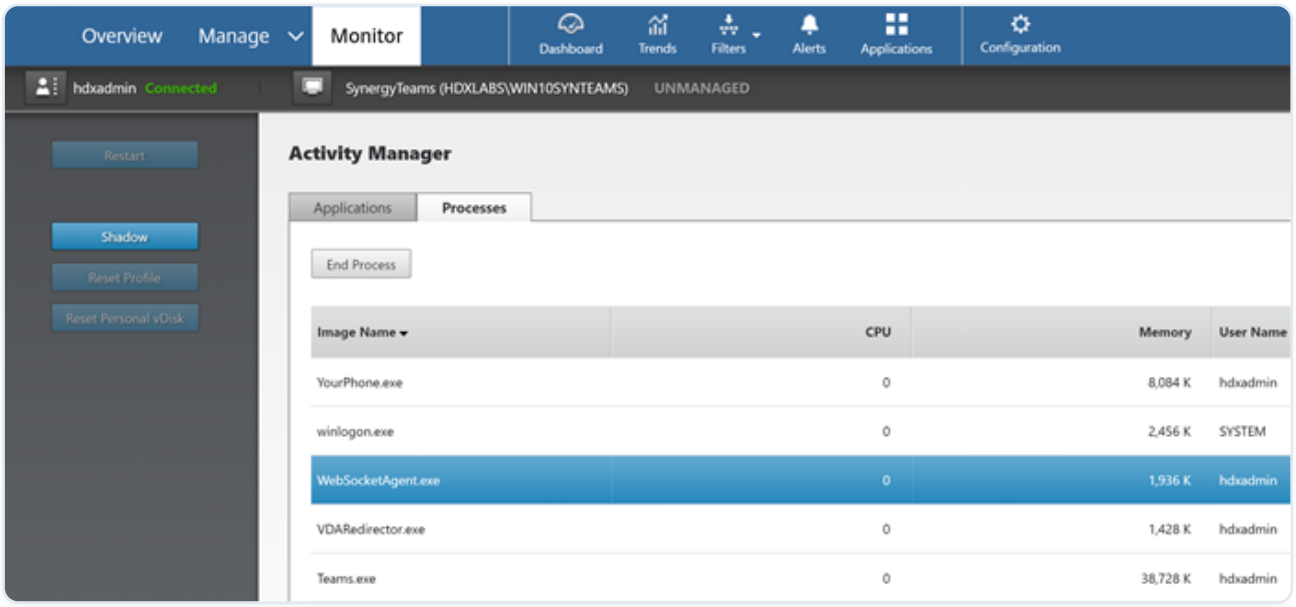
Informações adicionais

- Monitorar, solucionar problemas e dar suporte ao Microsoft Teams
- Implantar o aplicativo de desktop do Microsoft Teams na VM
- Instalar o Microsoft Teams usando MSI (seção Instalação VDI)
- Thin clients
- Ferramenta de Avaliação de Rede do Skype for Business
- Entender a coexistência e interoperabilidade do Microsoft Teams e do Skype for Business

Monitorar, solucionar problemas e dar suporte ao Microsoft Teams

Monitorar o Teams

Esta seção fornece diretrizes para monitorar a otimização do Microsoft Teams com HDX. Se você estiver executando no modo otimizado e `HdxRtcEngine.exe` estiver sendo executado na máquina cliente, um processo no VDA chamado `WebSocketAgent.exe` estará sendo executado na sessão. Use o **Activity Manager** no Director para ver o aplicativo.



Com a versão mínima 1912 do VDA, você pode monitorar chamadas ativas do Teams usando o Citrix HDX Monitor (versão mínima 3.11). O ISO do produto Citrix Virtual Apps and Desktops contém o `hdxmonitor.msi` mais recente na pasta `layout\image-full\Support\HDX Monitor`.

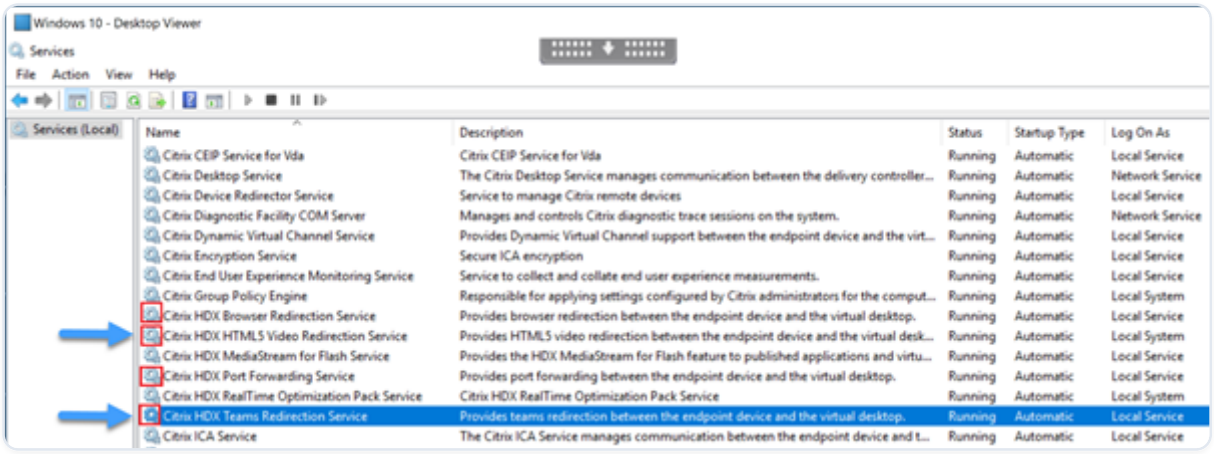
Para obter mais informações, consulte *Monitoramento* no artigo da Central de Conhecimento CTX253754.

Solucionar problemas

Esta seção fornece dicas de solução de problemas para questões que você pode encontrar ao usar a otimização para Microsoft Teams. Para obter mais informações, consulte CTX253754.

No Virtual Delivery Agent

Existem quatro serviços instalados por BCR_x64.msi. Apenas dois são responsáveis pelo redirecionamento do Microsoft Teams no VDA.



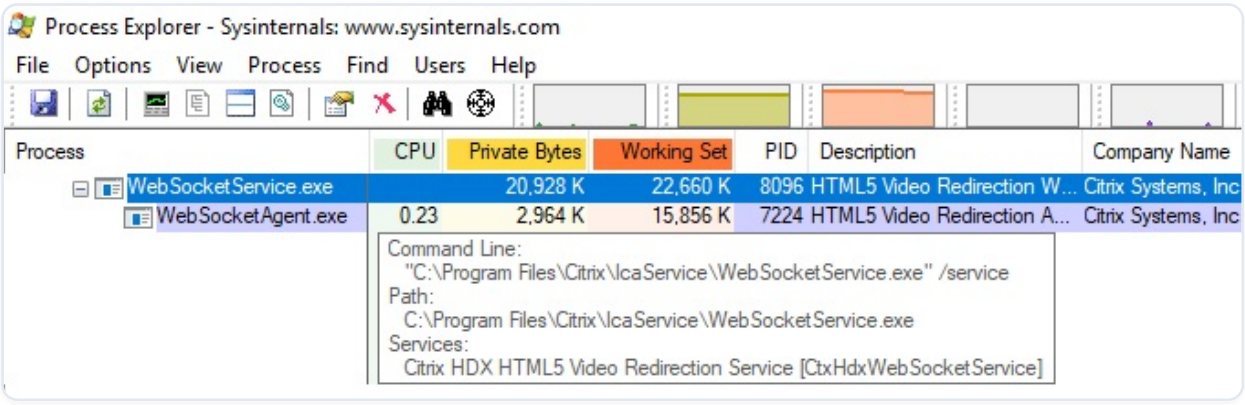
- O **Citrix HDX Teams Redirection Service** estabelece o canal virtual usado no Microsoft Teams. O serviço depende de CtxSvcHost.exe.
- O **Citrix HDX HTML5 Video Redirection Service** é executado como WebSocketService.exe, escutando em 127.0.0.1:9002 TCP. O WebSocketService.exe executa duas funções principais:

  i. A **terminação TLS para WebSockets seguros** recebe uma conexão WebSocket segura de vdiCitrixPeerConnection.js, que é um componente dentro do aplicativo Microsoft Teams. Você pode rastreá-lo com o Process Monitor. Para obter mais informações sobre certificados, consulte a seção "Redirecionamento de vídeo TLS e HTML5 e redirecionamento de conteúdo do navegador" em Comunicação entre Controller e VDA.

  Alguns softwares antivírus e de segurança de desktop interferem no funcionamento adequado de `WebSocketService.exe` e seus certificados. Embora o serviço Citrix HDX HTML5 Video Redirection possa estar sendo executado no console `services.msc`, o socket TCP localhost `127.0.0.1:9002` nunca está no modo de escuta, como visto no netstat. Tentar reiniciar o serviço faz com que ele trave ("Parando..."). Certifique-se de aplicar as exclusões adequadas para o processo `WebSocketService.exe`.



  ii. **Mapeamento da sessão do usuário.** Quando o aplicativo Microsoft Teams é iniciado, o WebSocketService.exe inicia o processo WebSocketAgent.exe na sessão do usuário no VDA. O WebSocketService.exe é executado na Sessão 0 como uma conta LocalSystem.



Você pode usar o **netstat** para verificar se o serviço WebSocketService.exe está em um estado de escuta ativo no VDA.

Execute `netstat -anob -p tcp` a partir de uma janela de prompt de comando elevada:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

Em uma conexão bem-sucedida, o estado muda para ESTABLISHED:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

Importante:

O WebSocketService.exe escuta em dois soquetes TCP, 127.0.0.1:9001 e 127.0.0.1:9002. A porta 9001 é usada para redirecionamento de conteúdo do navegador e redirecionamento de vídeo HTML5. A porta 9002 é usada para redirecionamento do Microsoft Teams. Certifique-se de que não haja configurações de proxy no sistema operacional Windows do VDA que possam impedir uma comunicação direta entre Teams.exe e WebSocketService.exe. Às vezes, quando você configura um proxy explícito no Internet Explorer 11 (**Opções da Internet > Conexões > Configurações da LAN > Servidor Proxy**), as conexões podem fluir através de um servidor proxy atribuído. Verifique se a opção **Ignorar servidor proxy para endereços locais** está marcada ao usar uma configuração de proxy manual e explícita.

Locais e descrições dos serviços

SERVIÇO	CAMINHO PARA O EXECUTÁVEL NO SO WINDOWS SERVER	FAZER LOGON COMO	DESCRIÇÃO
Serviço de Redirecionamento de Vídeo HTML5 do Citrix	"C:\Arquivos de Programas (x86)\Citrix\System32\WebSocketService.exe" /service	Conta do Sistema Local	Fornece vários serviços multimídia HDX com a estrutura inicial necessária para realizar o redirecionamento de mídia entre o desktop virtual e o dispositivo de endpoint.
Serviço de Redirecionamento de Navegador HDX do Citrix	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	Esta conta (serviço local)	Fornece redirecionamento de conteúdo do navegador entre o dispositivo de endpoint e o desktop virtual.
Serviço de Encaminhamento de Porta do Citrix	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	Esta conta (serviço local)	Fornece encaminhamento de porta entre o dispositivo de endpoint e o desktop virtual para redirecionamento de conteúdo do navegador.
Serviço de Redirecionamento de Teams HDX do Citrix	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	Conta do Sistema Local	Fornece redirecionamento do Microsoft Teams entre o dispositivo de endpoint e o desktop virtual.

Aplicativo Citrix Workspace™

No endpoint do usuário, o aplicativo Citrix Workspace para Windows instancia um novo serviço chamado HdxTeams.exe. Ele faz isso quando o Microsoft Teams é iniciado no VDA e o usuário tenta ligar ou acessar os periféricos na visualização automática. Se você não vir este serviço, verifique o seguinte:

1. Certifique-se de ter instalado no mínimo a versão 1905 do aplicativo Workspace para Windows. Você vê os binários HdxTeams.exe e webrpc.dll no caminho de instalação do aplicativo Workspace?
2. Se você validou a etapa 1, faça o seguinte para verificar se o HdxTeams.exe está sendo iniciado.
    a. Saia do Microsoft Teams no VDA.
    b. Inicie services.msc no VDA.
    c. Pare o Serviço de Redirecionamento de Equipes Citrix HDX.
    d. Desconecte a sessão ICA®.
    e. Conecte a sessão ICA.
    f. Inicie o Serviço de Redirecionamento de Equipes Citrix HDX.
    g. Reinicie o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX.
    h. Inicie o Microsoft Teams no VDA.
3. Se você ainda não vir o HdxTeams.exe sendo iniciado no endpoint do cliente, faça o seguinte:
    a. Reinicie o VDA.
    b. Reinicie o endpoint do cliente.

Suporte

A Citrix e a Microsoft dão suporte conjunto à entrega do Microsoft Teams a partir do Citrix Virtual Apps and Desktops™ usando a otimização para Microsoft Teams. Esse suporte conjunto é o resultado de uma colaboração próxima entre as duas empresas. Se você tiver contratos de suporte válidos e encontrar um problema com esta solução, abra um tíquete de suporte com o fornecedor cujo código você suspeita estar causando o problema. Ou seja, Microsoft para o Teams ou Citrix para os componentes de otimização.

A Citrix ou a Microsoft recebe o tíquete, avalia o problema e o encaminha conforme apropriado. Não há necessidade de você entrar em contato com a equipe de suporte de cada empresa.

Quando você tiver um problema, recomendamos que clique em **Ajuda > Relatar um Problema** na interface do usuário do Teams. Os logs do lado do VDA são compartilhados automaticamente entre a Citrix e a Microsoft para resolver problemas técnicos mais rapidamente.

Coletando logs

Os logs do mecanismo de mídia HDX podem ser encontrados na máquina do usuário (não no VDA). Em caso de problemas, certifique-se de anexar os logs ao seu caso de suporte.

Logs do Windows:

Você pode localizar os logs do Windows em %TEMP% dentro da pasta **HDXTeams** (AppData/Local/Temp/HDXTeams ou AppData/Local/Temp/HdxRtcEngine). Procure um arquivo .txt chamado webrpc_Day_Month_timestamp_Year.txt. Se você estiver usando versões mais recentes do aplicativo Citrix Workspace, por exemplo, Citrix Workspace app 2009.5 ou posterior, armazene os logs em AppData\Local\Temp\HdxRtcEngine.

Cada sessão cria uma pasta separada para os logs.

Logs do Mac:

1. Log VDWEBRTC - registra a execução do canal virtual.

   Localização: `/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`
2. Log HdxRtcEngine - registra a execução dos processos no HdxRtcEngine.

   Localização: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   O log HdxRtcEngine está habilitado por padrão.
3. Logs Webrpc - são os logs mais importantes que registram a execução do encerramento da biblioteca webrtc.

   Localização: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Logs do Linux:

Você pode localizar os logs do Linux nas pastas `/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`. Log do Webrtc: `/tmp/webrpc/<current date>/webrtc.log` Log do Kernel: `/var/log/syslog`

Logs ICE/STUN/TURN/:

Ao estabelecer uma chamada, estas quatro fases ICE são necessárias:

- Coleta de candidatos
- Troca de candidatos
- Verificações de conectividade (solicitações de vinculação STUN)
- Promoção de candidatos

Nos logs HdxRtcEngine.exe, as seguintes entradas são as entradas relevantes do Interactive Connectivity Establishment (ICE). Essas entradas devem estar presentes para que a configuração de uma chamada seja bem-sucedida. Veja o seguinte trecho de exemplo para o estágio de coleta:

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
```

```
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

Se houver vários candidatos ICE, a ordem de preferência é:

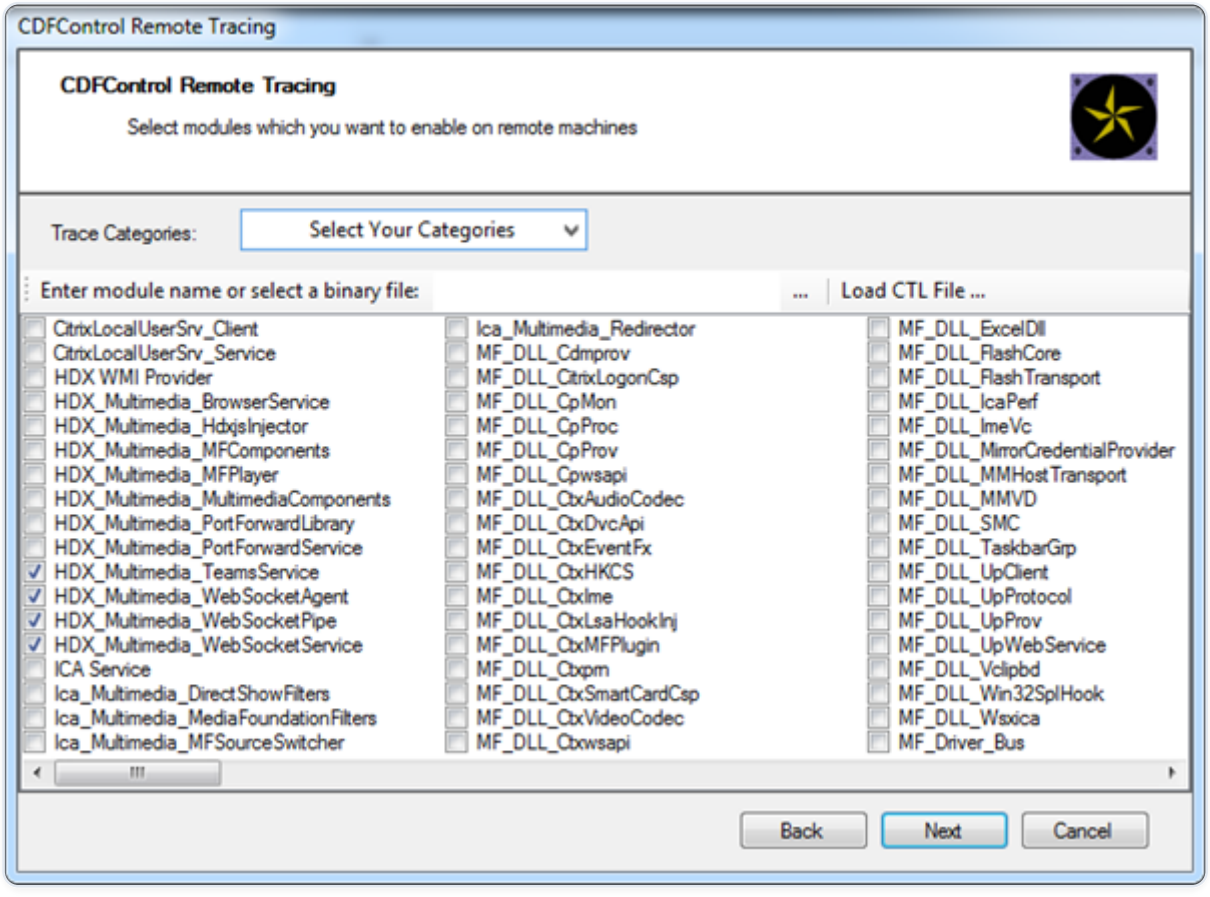
1. Servidor

2. reflexivo de par
3. reflexivo do servidor
4. retransmissão de transporte

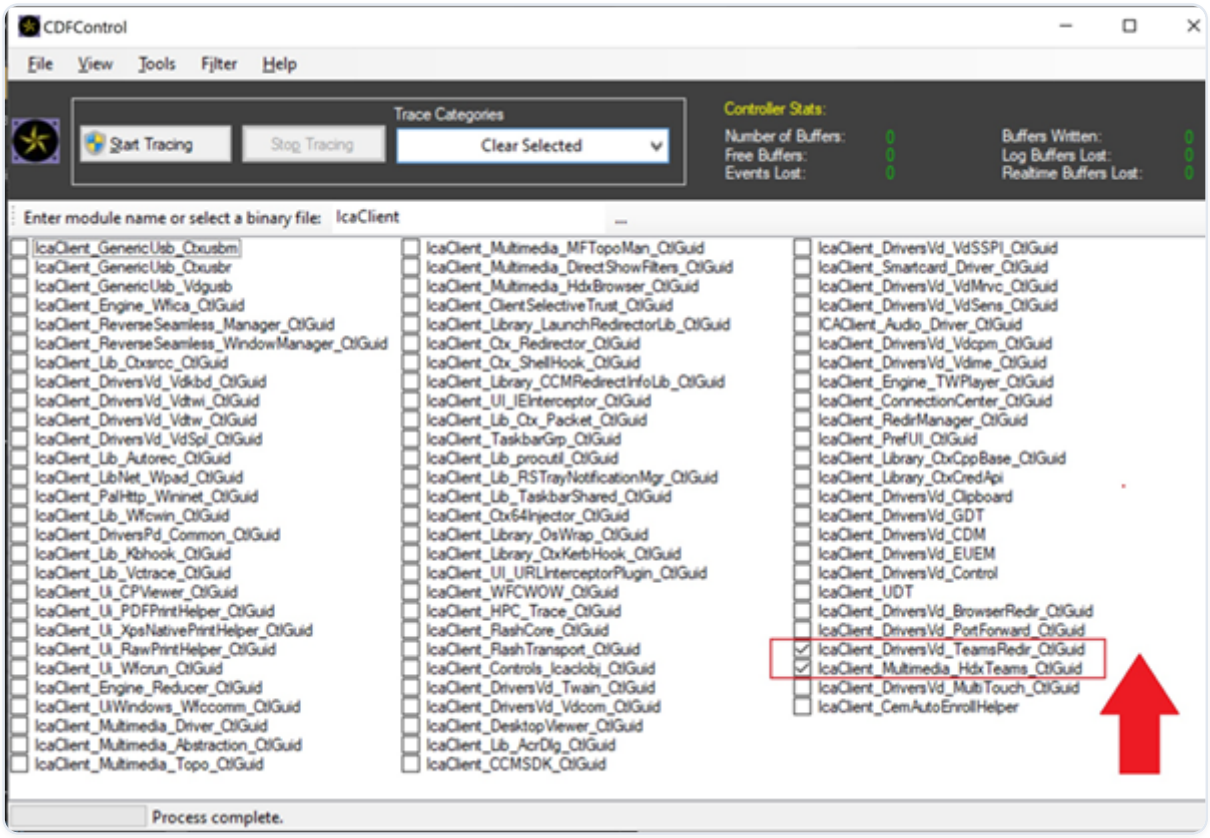
Se você encontrar um problema e puder reproduzi-lo consistentemente, recomendamos que você clique em **Ajuda > Relatar um problema** no Teams. Os logs são compartilhados entre a Citrix e a Microsoft para resolver problemas técnicos, caso você tenha aberto um caso com a Microsoft. A captura de rastreamentos CDF antes de entrar em contato com o Suporte Citrix também é benéfica. Para obter mais informações, consulte o artigo da Central de Conhecimento CDFcontrol.

Para recomendações sobre a coleta de rastreamentos CDF, consulte o artigo da Central de Conhecimento Recomendações para Coletar os Rastros CDF.

Rastreamentos CDF do lado do VDA - Habilite os seguintes provedores de rastreamento CDF:



Rastreamentos CDF do lado do aplicativo Workspace - Habilite os seguintes provedores de rastreamento CDF:



- IcaClient_DriversVd_TeamsRedir (opcional)
- IcaClient_Multimedia_HdxTeams (requer o aplicativo Citrix Workspace 2012 ou posterior)

Redirecionamento de Mídia do Windows

O redirecionamento de Mídia do Windows controla e otimiza a forma como os servidores entregam áudio e vídeo em streaming aos usuários. Ao reproduzir os arquivos de tempo de execução de mídia no dispositivo cliente em vez do servidor, o redirecionamento de Mídia do Windows reduz os requisitos de largura de banda para a reprodução de arquivos multimídia. O redirecionamento de Mídia do Windows melhora o desempenho do Windows Media Player e de players compatíveis executados em desktops virtuais do Windows.

Se os requisitos para a busca de conteúdo do lado do cliente do Windows Media não forem atendidos, a entrega de mídia usará automaticamente a busca do lado do servidor. Este método é transparente para os usuários. Você pode usar o Citrix Scout para realizar um rastreamento do Citrix Diagnosis Facility (CDF) de HostMMTransport.dll para determinar o método usado. Para obter mais informações, consulte Citrix Scout.

O redirecionamento de Mídia do Windows intercepta o pipeline de mídia no servidor host, captura os dados de mídia em seu formato compactado nativo e redireciona o conteúdo para o dispositivo cliente. O dispositivo cliente então recria o pipeline de mídia para descompactar e renderizar os dados de mídia recebidos do servidor host. O redirecionamento de Mídia do Windows funciona

bem em dispositivos cliente que executam um sistema operacional Windows. Esses dispositivos possuem a estrutura multimídia necessária para reconstruir o pipeline de mídia como existia no servidor host. Clientes Linux usam estruturas de mídia de código aberto semelhantes para reconstruir o pipeline de mídia.

A configuração de política **Redirecionamento de Mídia do Windows** controla esse recurso e está **Permitida** por padrão. Geralmente, essa configuração aumenta a qualidade de áudio e vídeo renderizada do servidor para um nível comparável ao conteúdo reproduzido localmente em um dispositivo cliente. Em casos raros, a reprodução de mídia usando o redirecionamento de Mídia do Windows parece pior do que a mídia renderizada usando a compactação ICA® básica e áudio regular. Você pode desabilitar esse recurso adicionando a configuração **Redirecionamento de Mídia do Windows** a uma política e definindo seu valor como **Proibido**.

Para obter mais informações sobre as configurações de política, consulte Configurações de política de multimídia.

Limitação:

Ao usar o Windows Media Player e as Extensões de Áudio e Vídeo Remotas (RAVE) ativadas dentro de uma sessão, uma tela preta pode aparecer. Essa tela preta pode aparecer se você clicar com o botão direito do mouse no conteúdo do vídeo e selecionar **Sempre mostrar Em Reprodução no topo**.

Gerenciador de Plug-ins de Canal Virtual

Introdução

O gerenciador de plug-ins de canal virtual foi projetado para implantar plug-ins em endpoints de cliente para aplicativos especificados. O gerenciador de plug-ins detecta aplicativos específicos em execução no VDA e solicita ao usuário que instale o plug-in no endpoint para obter a melhor experiência ao executar o aplicativo.

Os usuários podem optar por instalar o plug-in, ignorá-lo ou negar a instalação. O gerenciador de plug-ins oferece flexibilidade para gerenciar os plug-ins em todos os endpoints - gerenciados ou não gerenciados.

Por exemplo: O Microsoft Teams possui uma nova arquitetura (Otimização SlimCore), que requer que um plug-in seja instalado nos endpoints para que a otimização funcione. O gerenciador de plug-ins de canal virtual pode implantar os plug-ins em seus endpoints. Para obter mais informações, consulte nova solução VDI para Teams

Requisitos do Sistema

A seguir estão os requisitos mínimos para o gerenciador de plug-ins de canal virtual.

- Virtual Desktop Agent (VDA)
  - 2411 CR
  - 2402 LTSR CU2
- DDC
  - Cloud 121 Release
  - 2407 CR
  - 2402 LTSR CU1
- Citrix Workspace™ App (Citrix Workspace App)
  - Citrix Workspace App para Windows 2409

> **Observação:**

> Este recurso é atualmente aplicável a endpoints Windows.

Aplicativos suportados

- Os aplicativos atualmente suportados estão listados abaixo:
  - Microsoft Teams - Consulte nova solução VDI para Teams

Visão geral do Gerenciador de Plug-ins de Canal Virtual

Compreendendo o Recurso

A Citrix® entende que os ambientes dos clientes podem ser complexos e que a implantação de um plug-in em endpoints gerenciados e não gerenciados exige um esforço significativo. Este recurso foi projetado para simplificar o processo.

Este recurso inclui dois componentes: um no lado do VDA (processo detector) e outro no lado do Citrix Workspace™ App (processo instalador). Quando os administradores atendem aos pré-requisitos mencionados acima, como habilitar políticas, fazer entradas de registro e especificar um aplicativo para monitorar:

- O processo detector do lado do VDA monitora o lançamento do aplicativo pelo usuário final assim que ele faz logon na área de trabalho virtual
- O processo detector informa o lado do Citrix Workspace App para solicitar ao usuário que instale o plug-in necessário para otimizar o aplicativo especificado
- Os usuários recebem um pop-up em sua tela com breves detalhes sobre o plug-in. Os usuários podem optar por instalar o plug-in, ignorar ou optar por nunca instalá-lo
    - Se os usuários ignorarem o processo de instalação, eles não verão o pop-up novamente nessa sessão. O prompt de instalação aparecerá ao reconectar a sessão.
    - Se os usuários optarem por nunca instalar o plug-in, a escolha será registrada em seu perfil de usuário para visibilidade do administrador.
- Se os usuários optarem por instalar o plug-in, o lado do Citrix Workspace App fará o download e instalará o plug-in no endpoint.
    - Após a instalação bem-sucedida, o usuário receberá uma mensagem para reconectar a sessão para que o plug-in entre em vigor. O usuário pode optar por fazer isso imediatamente ou fechar a mensagem de sucesso e reconectar mais tarde.
    - Se a instalação falhar, o usuário verá uma mensagem de erro e a falha será registrada para visibilidade do administrador.

Configuração do Gerenciador de Plug-ins de Canal Virtual

Implantação

1. Verifique se a política de redirecionamento do Microsoft Teams está ativada: Consulte política de redirecionamento do Microsoft Teams para obter mais detalhes.

   Esta política deve ser ativada independentemente do aplicativo que está sendo monitorado. No futuro, se mais aplicativos forem suportados e você quiser monitorar esses aplicativos em vez do Microsoft Teams, esta política ainda deverá ser ativada. Observe que esta política é ativada por padrão.

2. A política do gerenciador de plug-ins de canal virtual deve ser ativada: Consulte configurações da política do gerenciador de plug-ins de canal virtual para obter instruções detalhadas sobre como ativar a política.

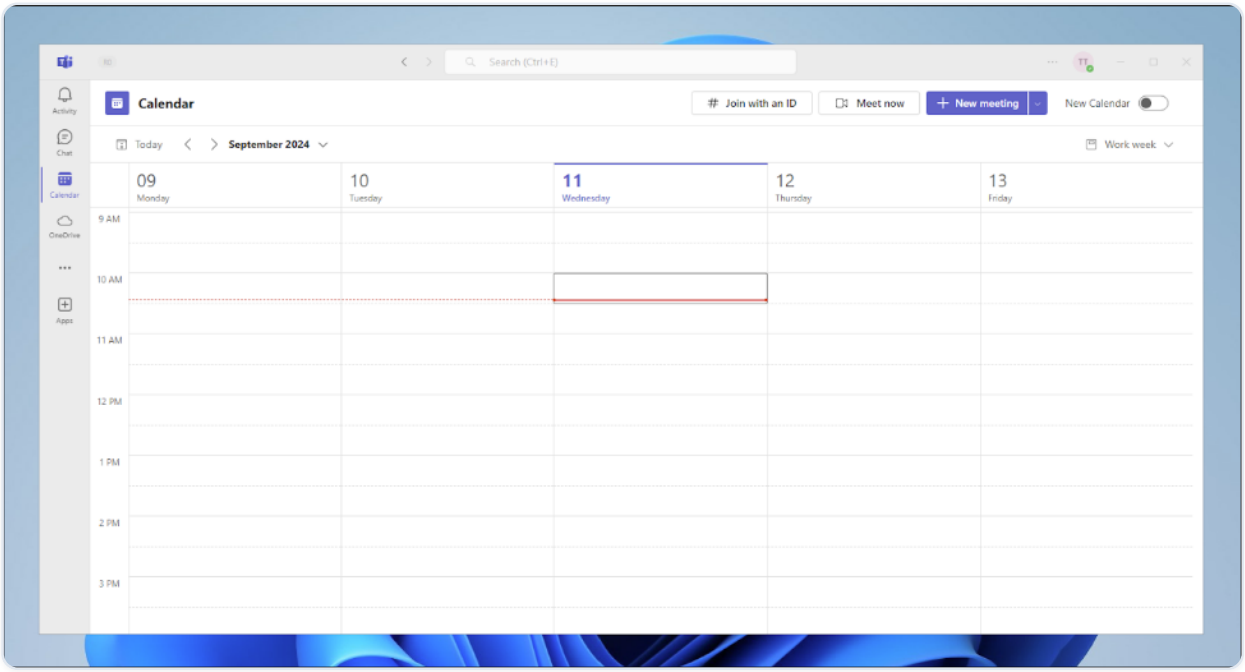
   Esta política está disponível nas Configurações de Política Multimídia no Citrix Studio. A ativação da política permite especificar o nome do aplicativo a ser monitorado, por exemplo, “Microsoft Teams”. Esta política é desativada por padrão.

3. O aplicativo Citrix Workspace™ deve ser instalado no modo de sistema.

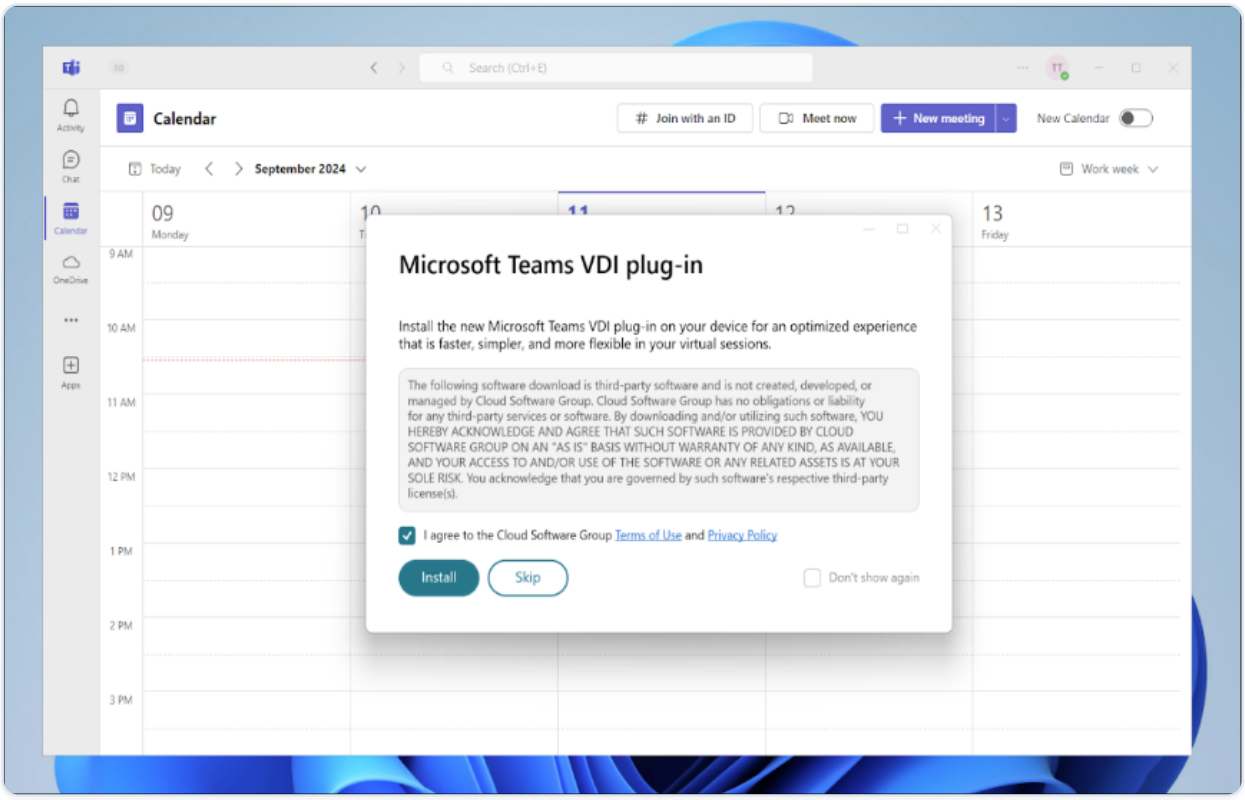
> **Nota:**
>
> Os plug-ins são baixados para o endpoint a partir da CDN de terceiros. Por exemplo, se você selecionar o Microsoft Teams, o plug-in será baixado da CDN da Microsoft. Portanto, o endpoint deve ter acesso à CDN de terceiros. Caso contrário, a instalação do plug-in falhará.

Procedimento

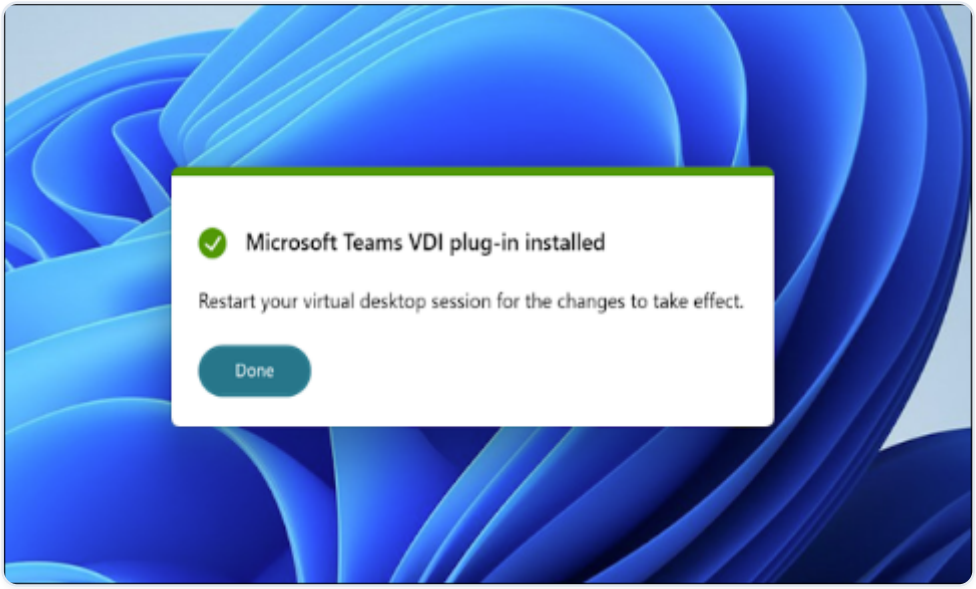
1. O usuário inicia o aplicativo na sessão Citrix. Por exemplo, Microsoft Teams.



2. O usuário recebe um pop-up para instalar o plug-in VDI do Teams no endpoint para uma melhor experiência. O pop-up aparece acima da sessão e não dentro da sessão, pois o plug-in será instalado no endpoint.



3. O usuário clica no botão de instalação e o plug-in é instalado. Os usuários precisam reiniciar a sessão da área de trabalho virtual para que as alterações entrem em vigor.



Problemas Conhecidos e Limitações

- No VDA 2407, a seguinte configuração de registro precisa ser definida como 1 no VDA, além da política, para que o recurso seja ativado. Essa configuração de registro é automaticamente permitida e não precisa ser configurada a partir do VDA 2411.

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

Name: EnableAppDetector Type: DWORD`

- Mais limitações a serem adicionadas

Otimização do SDK de Comunicações Unificadas

Introdução

O Citrix Virtual Apps and Desktops permite que você entregue aplicativos aos seus usuários em uma ampla variedade de dispositivos de endpoint. Muitos desses aplicativos incluem recursos de comunicação em tempo real (RTC), como conferência de áudio e vídeo. No entanto, desafios podem surgir ao entregar esses aplicativos em um ambiente virtualizado. Os métodos de entrega tradicionais roteiam fluxos de mídia (áudio/vídeo) do dispositivo cliente para o servidor VDI no data center antes de enviá-los de volta para o endpoint. Esse "hairpinning" introduz tráfego desnecessário e sobrecarga de processamento no servidor, especialmente para chamadas de áudio e vídeo que consomem muita largura de banda.

O Citrix Unified Communications SDK (UCSDK) é uma tecnologia que permite aos fornecedores de tecnologia otimizar esses aplicativos RTC para uso em ambientes Citrix. Quando um aplicativo é otimizado, ele pode fornecer uma experiência de usuário que corresponde ou até excede a do aplicativo em execução em um desktop local. No mundo de hoje, a comunicação em tempo real sem interrupções é essencial para a produtividade e colaboração. Ao usar aplicativos em um ambiente virtual, é crucial que as chamadas de áudio e vídeo, o compartilhamento de tela e outros recursos de comunicação funcionem tão bem quanto funcionariam em um desktop local. Aplicativos otimizados oferecem essa experiência.

Esta documentação do produto detalha tudo o que é necessário para que os clientes Citrix aprendam e implementem aplicativos otimizados com o UCSDK.

Como funciona

A Citrix oferece um método de entrega otimizado para aplicativos de comunicação em tempo real dentro de VDIs. Essa abordagem utiliza o Unified Communications SDK (UCSDK) para dividir o aplicativo virtualizado em duas partes:

- **Interface do Usuário (UI):** A interface do usuário permanece dentro do host virtual, exibida de forma transparente dentro do desktop virtual ou da janela do aplicativo.
- **Mecanismo de Mídia:** As tarefas de processamento de mídia (codificação/decodificação de áudio e vídeo) são descarregadas para o dispositivo local do usuário. Isso minimiza a carga do servidor e otimiza o uso da rede.

Normalmente, a Citrix oferece o UCSDK a fornecedores de tecnologia no espaço de comunicações em tempo real e trabalha com eles para integrar o UCSDK nesses aplicativos. Uma vez integrado, qualquer cliente Citrix que use um aplicativo otimizado com UCSDK terá uma experiência aprimorada. O Citrix UCSDK também pode ser consumido por clientes Citrix em casos onde um aplicativo interno personalizado está sendo construído. Na maioria dos casos, no entanto, os clientes não precisam consumir e desenvolver com o UCSDK – eles apenas precisam configurar o ambiente Citrix e o aplicativo para obter uma experiência otimizada.

> **Nota:**
>
> Referências ao Citrix WebRTC SDK (ou) a um aplicativo otimizado com HDX™ indicam integração com o Citrix UCSDK e podem ser usadas de forma intercambiável.

Novidades

O UCSDK 4.1.0 é a versão mais recente geralmente disponível que os fornecedores de tecnologia podem integrar. Além disso, há mais duas versões suportadas – UCSDK 4.0.2 e UCSDK 3.1.0. Novos recursos são introduzidos com as versões do UCSDK, e os fornecedores de tecnologia precisam garantir a atualização do SDK para que os clientes recebam os recursos. Dessa forma, os clientes Citrix podem se concentrar apenas na atualização dos componentes Citrix necessários para obter novos recursos.

Com o lançamento do UCSDK 4.1.0, estamos introduzindo aprimoramentos críticos na experiência do usuário e recursos totalmente novos que permitirão uma integração mais profunda com os produtos dos parceiros e mais valor para nossos clientes.

Novos Recursos

- **Gravação de Tela do Ponto de Extremidade UCSDK (Prévia Técnica):** Abordando uma lacuna fundamental na gravação de conformidade, as novas APIs do UCSDK agora podem capturar conteúdo no ponto de extremidade, mesmo quando os aplicativos estão sendo executados dentro do VDI. Este recurso, atualmente em prévia para pontos de extremidade Windows, permite que fornecedores de tecnologia aprimorem seus aplicativos para oferecer suporte à gravação de tela do ponto de extremidade no Citrix. Observe que este recurso está focado no aprimoramento de aplicativos de fornecedores e é diferente da gravação de sessão do Citrix.
- **Tratamento de Reconexão de Sessão:** Um aprimoramento crítico no Bootstrap melhora significativamente a experiência do aplicativo de navegador, aproximando-a da de aplicativos

de desktop baseados em Electron. Aplicativos baseados em navegador usando Bootstrap agora podem manipular dinamicamente desconexões de sessão do Citrix, proporcionando uma experiência de usuário perfeita para os usuários finais.

- **Suporte para Novos métodos:** Adicionado suporte para reiniciar a coleta ICE e suporte para `iceCandidatePoolSize` em `RTCConfiguration`.
- **Melhor Tratamento de Erros e Melhorias de Conformidade:** Conformidade aprimorada com a especificação WebRTC para `getUserMedia`. `getStats()` aprimorado para `CitrixPeerConnection`, `RtpSender` e `RtpReceiver` para retornar um relatório vazio em vez de nulo em condições de erro.

As versões totalmente compatíveis para UCSDK 4.1.0 incluem:

- Citrix Aplicativos Virtuais e Desktops™ 2503
- Citrix Workspace™ App para Windows 2503
- Citrix Workspace App para Mac 2503
- Citrix Workspace App para Linux 2503
- A versão mais recente do ChromeOS/HTML5.

> **Nota:**

> Os clientes Citrix podem entrar em contato com fornecedores de tecnologia para atualizar o SDK (ou) adicionar suporte a recursos específicos, caso existam casos de uso que possam ser alcançados com os recursos recém-introduzidos.

Principais Benefícios

Ao usar aplicativos otimizados com o Citrix UCSDK, você pode esperar:

- Desempenho aprimorado do processamento de mídia ao descarregar a codificação/decodificação de mídia intensiva em processador do Citrix Virtual Delivery Agent (VDA) para o endpoint do cliente, aumentando a capacidade de resposta geral para os usuários finais.
- Uso reduzido de CPU e largura de banda no Citrix VDA, permitindo que a TI suporte mais usuários simultâneos por host e que as empresas dimensionem as implantações de desktop virtual Citrix de forma econômica.

- Menor custo total de propriedade para as empresas, pois os endpoints otimizados estendem a vida útil dos desktops virtuais legados e reduzem as necessidades de infraestrutura de host, diminuindo assim os gastos de capital e os custos operacionais ao longo do tempo.
- Suporte para plataformas de endpoint Windows, Mac, Linux, ChromeOS e HTML5.

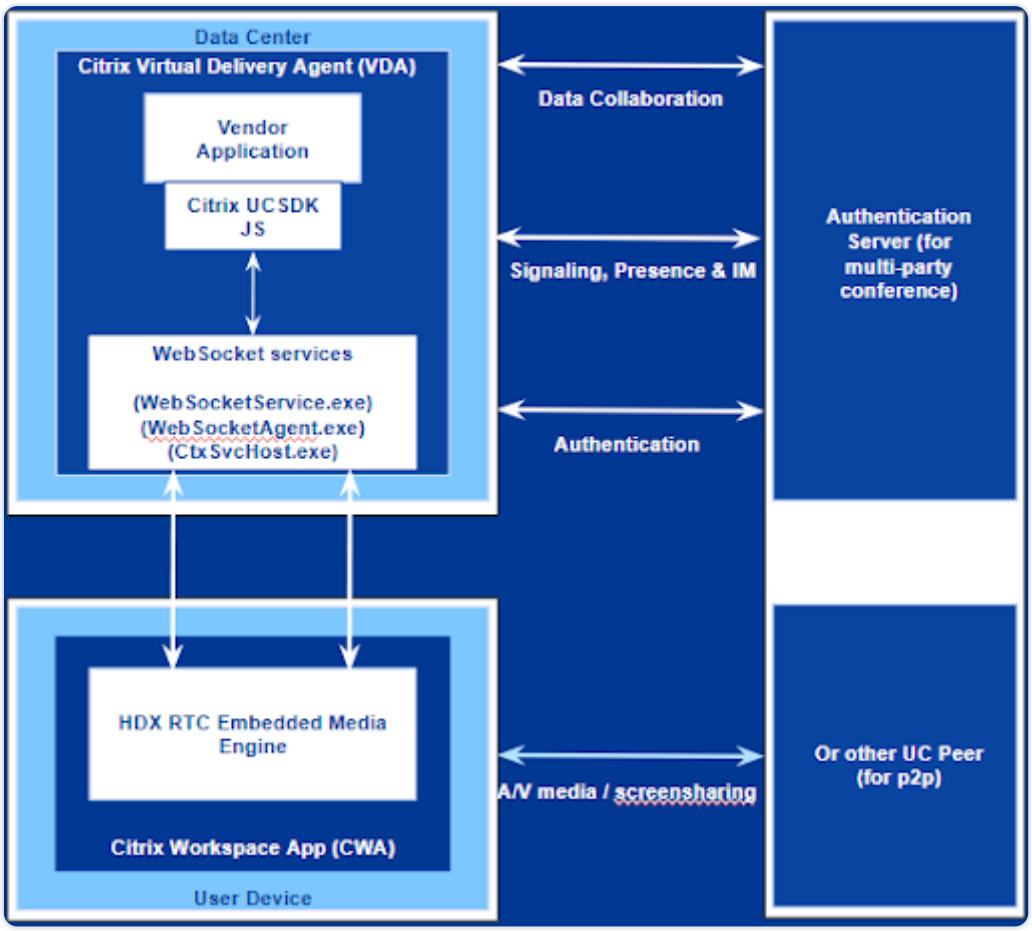
Casos de Uso

O UCSDK foi desenvolvido especificamente para otimizar aplicativos de comunicação em tempo real que aderem ao padrão WebRTC. Aqui estão os principais cenários e os tipos de aplicativos baseados em WebRTC que podem / já usam o UCSDK.

- **Contact Center as a Service (CCaaS) / Plataformas de Contact Center na Nuvem:** Gerenciam principalmente as interações com os clientes em vários canais, otimizando os fluxos de trabalho dos agentes.
    - Exemplos: Amazon Connect, Twilio, Avaya Experience Platform, Talkdesk, Content Guru
- **Unified Communications as a Service (UCaaS) / Comunicações Empresariais na Nuvem:** Integram voz, vídeo, mensagens de equipe e presença para uma comunicação empresarial abrangente.
    - Exemplos: Ring Central, 8x8, Intermedia, Alcatel-Lucent Rainbow
- **Communications Platform as a Service (CPaaS):** Fornecem APIs para incorporar recursos de comunicação em tempo real diretamente em aplicativos personalizados.
    - Exemplos: Twilio, Ribbon Communications
- **Videoconferência e Colaboração Empresarial:** Plataformas dedicadas para reuniões de vídeo de alta qualidade, conferências e recursos avançados de colaboração.
    - Exemplo: Pexip
- **Comunicações para Negociação Financeira:** Projetadas para as necessidades de comunicação exclusivas, de alto desempenho e em conformidade dos mercados financeiros.
    - Exemplo: IPC Unigy
- **Plataformas Virtuais de Aprendizagem e Treinamento:** Projetadas para experiências interativas e de alta qualidade em salas de aula e treinamentos virtuais.
    - Exemplo: Vitero

A base WebRTC subjacente do Citrix UCSDK significa que suas capacidades de otimização podem se estender a qualquer aplicativo de comunicação baseado em WebRTC. Isso abre as portas para otimizar uma ampla gama de aplicativos que utilizam WebRTC para interações em tempo real, mesmo que não estejam atualmente listados como otimizados com o UCSDK. Incentivamos os clientes a entrar em contato com a Citrix com quaisquer casos de uso ou aplicativos que desejam ver otimizados.

Arquitetura do UCSDK



- Aplicativo do fornecedor: Este pode ser qualquer aplicativo de comunicação em tempo real de terceiros, baseado em desktop ou navegador, que tenha integrado o UCSDK.
- UCSDK JS: O UCSDK JS fornece as APIs que os aplicativos do fornecedor utilizam para descarregar o áudio/vídeo para o endpoint.
- HdxRtcEngine: Este é o mecanismo de mídia WebRTC incorporado no Citrix Workspace App que processa e gerencia a chamada de áudio/vídeo descarregada.

Uma vez que o SDK é carregado e usado, o processo `HdxRtcEngine.exe` é iniciado no endpoint do cliente se o redirecionamento for bem-sucedido. Uma vez que `HdxRtcEngine.exe` é iniciado no endpoint do cliente, quaisquer dados de sinalização e payload fluem do Citrix VDA para o

endpoint do cliente, chegam à nuvem, retornam ao endpoint do cliente e, em seguida, são encaminhados para o VDA. Por exemplo, um ciclo completo de fluxo poderia ser:

```
Vendor App -> CitrxWebrtc.js SDK -> Citrix VDA components -> Citrix Client Endpoint components -> Cloud -> Citrix Client Endpoint components -> Citrix VDA components -> CitrxWebrtc.js SDK -> Vendor App
```

Requisitos do Sistema

Os requisitos do sistema indicam as várias versões dos componentes Citrix necessários com a versão mais recente do UCSDK - 4.1.0. Para detalhes de compatibilidade para versões mais antigas do SDK e requisitos de recursos específicos, consulte a tabela Matriz de Versões e Recursos abaixo.

> **Nota:**

> Para que os clientes utilizem qualquer recurso adicionado ao UCSDK – certifique-se de que o aplicativo do fornecedor integrou a versão apropriada do UCSDK e habilitou o recurso, e utilize as versões apropriadas de VDA e CWA em seu ambiente.

Versões Totalmente Compatíveis

Versões totalmente compatíveis indicam que, ao usar essas versões dos componentes Citrix juntamente com a versão mais recente do UCSDK, os clientes podem aproveitar todos os recursos disponíveis. Para a versão mais recente atual do UCSDK – 4.1.0, as versões totalmente compatíveis dos componentes Citrix são as seguintes:

- **Citrix Virtual Apps e Desktops:** 2503
- **Citrix Workspace App Windows:** 2503
- **Citrix Workspace App Mac:** 2503
- **Citrix Workspace App Linux:** 2503
- **Citrix Workspace App ChromeOS/HTML5:** Versão mais recente

Configuração

A funcionalidade do recurso UCSDK depende de três fatores: a versão do UCSDK que o fornecedor integrou e os recursos que o fornecedor habilitou, o Citrix Virtual Apps and Desktops e a versão do aplicativo Citrix Workspace em uso.

No lado Citrix, certifique-se de que o seguinte esteja configurado para que o aplicativo otimizado possa ser otimizado:

1. Certifique-se de que a política de redirecionamento do Microsoft Teams esteja ativada. Consulte Configurações da Política Multimídia para obter mais informações. Observe que esta política está ATIVADA por padrão.
2. Aplicativos de terceiros baseados em Electron ou navegador que utilizam o SDK `CitrixWebrtc.js` não são suportados por padrão. O `CtxHdxWebSocketService` (`WebSocketService.exe`) não permitirá conexões de aplicativos que não estejam na lista de permissões. O nome do executável binário do aplicativo desejado deve ser adicionado a uma chave de registro de lista de permissões.

No VDA

- Criar um Caminho de Chave: `HKLM\Software\WOW6432Node\Citrix\WebSocketService`
- Nome da Chave: `ProcessWhitelist`
- Tipo: `MULTISZ`
- Valor da Chave: `Mytestapp.exe`

Se você tiver vários aplicativos, digite cada aplicativo em uma nova linha. Não copie e cole de um arquivo de texto nem insira vírgulas. Certifique-se de que o nome fornecido corresponda ao nome do executável do aplicativo. Este valor de registro não diferencia maiúsculas de minúsculas.

Se o aplicativo for acessado por meio de um navegador em vez de um aplicativo de desktop completo, então você precisa permitir, por exemplo, `chrome.exe` no valor do registro.

Depois que o registro acima for configurado com sucesso, reinicie o VDA ou reinicie `CtxHdxWebSocketService` para finalizar a configuração da Lista de Permissões.

No Cliente

Nenhuma configuração é necessária. Basta instalar o aplicativo Citrix Workspace.

Cada fornecedor pode ter um nome de aplicativo muito específico. Portanto, consulte a documentação do fornecedor vinculada na seção Suporte ao Fornecedor Atual para determinar qual nome de aplicativo deve ser permitido no WebSocketService.

Versões e Matriz de Recursos

Como as atualizações de versão ocorrem com frequência, consulte as páginas de ciclo de vida do produto Citrix Virtual Apps and Desktops e Citrix Workspace app para garantir que uma versão específica seja suportada. Para muitos dos recursos mais antigos, as versões mencionadas na tabela são as últimas versões de Lançamento Atual (CR) suportadas no momento da redação deste documento.

RECURSO	VERSÃO DO UCSDK	VDA	CWA WINDOWS	CWA MAC	CWA LINUX	CWA CHROME OS/ HTML5
Áudio / Vídeo (p2p e conferência)	3.1.0	2203 LTSR CU Mais Recente / 2311 CR	2402 LTSR CU Mais Recente / 2311 CR	2311	2311	2312
Compartilhamento de tela	3.1.0	2203 LTSR CU Mais Recente / 2311 CR	2402 LTSR CU Mais Recente / 2311 CR	2311	2311	2312
DTMF	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Suporte a Servidor Proxy	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Compartilhamento de apps	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	N/A

RECURSO	VERSÃO DO UCSDK	VDA	CWA WINDOWS	CWA MAC	CWA LINUX	CWA CHROME OS/ HTML5
e911 Dinâmico	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Múltiplas Janelas	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Suporte ao Plano Unificado SDP	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Resolução de stream / Simulcast	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2312
Áudio Remoto (com Loop)	3.1.0	2203 LTSR Latest CU / 2311 CR	2402 LTSR Latest CU / 2311 CR	2311	2311	2405
UCSDK baseado em navegador (suporte a Bootstrap)	4.0.2	2407 CR	2402 LTSR Última CU / 2311 CR	2311	2311	2312

RECURSO	VERSÃO DO UCSDK	VDA	CWA WINDOWS	CWA MAC	CWA LINUX	CWA CHROME OS/ HTML5
Web HID API	4.0.2	2203 LTSR Última CU / 2311 CR	2409.10	2411	2411	2505
Web Audio API	4.0.2	2203 LTSR Última CU / 2311 CR	2405	2405	2405	N/A
Reiniciar ICE	4.1.0	2203 LTSR CU Mais Recente / 2311 CR	2503.2	2503	2503	2502.10
Gravação de Tela (Prévia)[1]	4.1.0	2503	2503.2	N/A	N/A	N/A

Nota:

Introduzimos uma nova política para gravação de tela, então você precisa da versão 2503 do delivery controller™, que vem com o CVAD 2503.

Suporte Atual do Fornecedor

Vários fornecedores terceirizados integraram o SDK de Comunicações Unificadas em seus produtos. A lista atual de fornecedores e sua documentação de suporte está listada abaixo:

FORNECEDOR	DOCUMENTAÇÃO
Amazon Connect	Otimizar áudio do Amazon Connect para desktops em nuvem Citrix
Ring Central	Usando o RingCentral em um ambiente Citrix VDI
Five9	Five9 WebRTC em Ambientes Citrix
Twilio	Twilio Flex no Citrix VDI
Avaya	Solução Avaya Experience Platform Public Cloud VDI para Citrix
8x8	Integração Citrix VDI com 8x8 Work para Desktop e Web
Content Guru	Integração Content Guru Citrix
Ribbon Communications	Ribbon Communications Citrix WebRTC SDK
Intermedia	Instalando Intermedia Unite em Citrix Virtual Apps and Desktops
Alcatel-Lucent Rainbow	Otimização Citrix para o Aplicativo de Desktop Rainbow
Talkdesk	Talkdesk Agent Workspace VDI Connect
IPC	IPC Unigy Soft Client Citrix VDI
Vitero	Vitero Inspire para Citrix VDI
Pexip	Implantando o aplicativo de desktop Connect em Citrix Pexip Infinity Docs

Solução de problemas

Para obter informações sobre solução de problemas, consulte Troubleshooting Guidance for Apps Optimized with Citrix Unified Communications SDK.

Problemas Conhecidos e Limitações

Esta seção documentará os problemas conhecidos e as limitações atuais à medida que forem reconhecidos.

Redirecionamento geral de conteúdo

O redirecionamento de conteúdo permite controlar se os usuários acessam informações usando aplicativos publicados em servidores ou usando aplicativos executados localmente em dispositivos de usuário.

Redirecionamento de pasta do cliente(/pt-br/citrix-daas/general-content-redirection/client-folder-redirection.html)

O redirecionamento de pasta do cliente altera a forma como os arquivos do lado do cliente são acessíveis na sessão do lado do host.

- Quando você habilita apenas o mapeamento de unidade do cliente no servidor, os volumes completos do lado do cliente são automaticamente mapeados para as sessões como links de Convenção Universal de Nomenclatura (UNC).
- Quando você habilita o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo de desktop Windows, a parte do volume local especificada pelo usuário é redirecionada.

Redirecionamento do host para o cliente(/pt-br/citrix-daas/general-content-redirection/bidirectional-content-redirection-configuration/host-to-client-redirection.html)

Considere usar o redirecionamento do host para o cliente para casos de uso incomuns específicos. Normalmente, outras formas de redirecionamento de conteúdo podem ser melhores. Oferecemos suporte a esse tipo de redirecionamento apenas em VDAs de SO de múltiplas sessões e não em VDAs de SO de sessão única.

Acesso a aplicativos locais e redirecionamento de URL(/pt-br/citrix-daas/general-content-redirection/laa-url-redirect.html)

O Acesso a Aplicativos Locais integra perfeitamente aplicativos Windows instalados localmente em um ambiente de desktop hospedado. Isso é feito sem a necessidade de alternar de um computador para outro.

A tecnologia HDX™ oferece **redirecionamento USB genérico** para dispositivos especiais que não possuem suporte otimizado ou onde ele é inadequado.

Redirecionamento de pasta do cliente

O redirecionamento de pasta do cliente muda a forma como os arquivos do lado do cliente são acessíveis na sessão do lado do host. Se você habilitar apenas o mapeamento de unidade do cliente no servidor, volumes completos do lado do cliente são automaticamente mapeados como links de Convenção Universal de Nomenclatura (UNC) para as sessões. Quando você habilita o redirecionamento de pasta do cliente no servidor e o usuário o configura no dispositivo do usuário, a parte do volume local especificada pelo usuário é redirecionada.

Apenas as pastas especificadas pelo usuário aparecem como links UNC dentro das sessões. Ou seja, em vez do sistema de arquivos completo no dispositivo do usuário. Se você desabilitar os links UNC através do registro, as pastas do cliente aparecem como unidades mapeadas dentro da sessão.

O redirecionamento de pasta do cliente é suportado apenas em máquinas Windows Single-session OS.

O redirecionamento de pasta do cliente para uma unidade USB externa não é salvo ao desconectar e reconectar o dispositivo.

Habilite o redirecionamento de pasta do cliente no servidor. Em seguida, no dispositivo cliente, especifique quais pastas redirecionar. O aplicativo que você usa para especificar as opções de pasta do cliente está incluído no aplicativo Citrix Workspace™ fornecido com esta versão.

Requisitos:

Para servidores:

- Windows Server 2019, edições Standard e Datacenter
- Windows Server 2016, edições Standard e Datacenter
- Windows Server 2012 R2, edições Standard e Datacenter

Para clientes:

- Windows 10, edições de 32 bits e 64 bits (versão mínima 1607)
- Windows 8.1, edições de 32 bits e 64 bits (incluindo a edição Embedded)
- Windows 7, edições de 32 bits e 64 bits (incluindo a edição Embedded)

Para habilitar o redirecionamento de pasta do cliente no servidor, consulte Redirecionamento de pasta do cliente na lista de recursos gerenciados através do registro.

No dispositivo do usuário, especifique quais pastas redirecionar:

1. Certifique-se de que a versão mais recente do aplicativo Citrix Workspace esteja instalada.
2. No diretório de instalação do aplicativo Citrix Workspace, inicie CtxCFRUI.exe.
3. Escolha o botão de opção **Personalizado** e adicione, edite ou remova pastas.
4. Desconecte e reconecte suas sessões para que a configuração entre em vigor.

Configuração de redirecionamento de conteúdo bidirecional

O redirecionamento de conteúdo bidirecional permite que URLs sejam redirecionadas do cliente para o servidor ou do servidor para o cliente, dependendo das configurações. Esta configuração de política substitui as três configurações a seguir, que estão obsoletas:

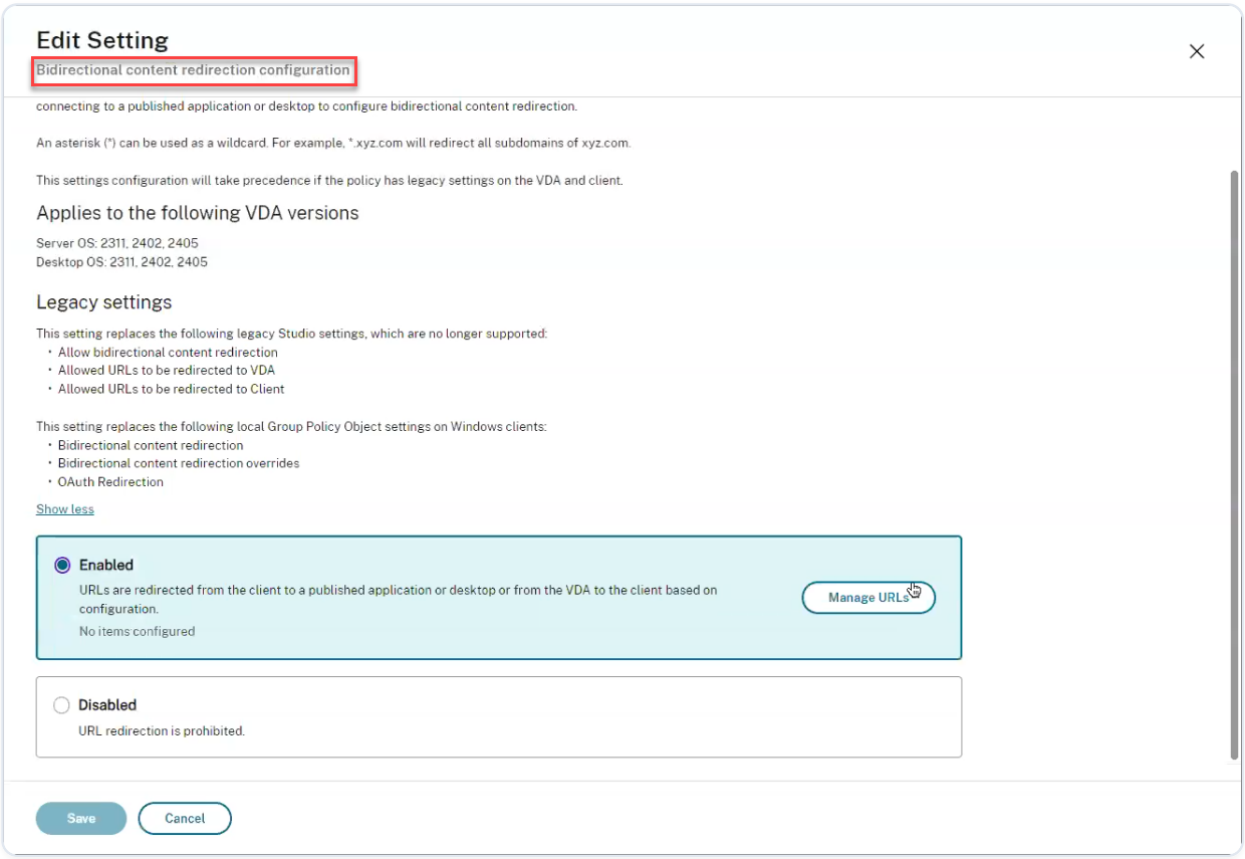
- Permitir redirecionamento de conteúdo bidirecional
- URLs permitidas para serem redirecionadas para o VDA
- URLs permitidas para serem redirecionadas para o Cliente

Ele também substitui as três configurações de GPO locais a seguir em clientes Windows:

- Redirecionamento de conteúdo bidirecional
- Substituições de redirecionamento de conteúdo bidirecional
- Redirecionamento OAuth

Se esta configuração for configurada, ela terá precedência sobre as configurações legadas no Studio e no cliente. Para configurar a política de redirecionamento de conteúdo bidirecional, faça o seguinte:

1. No Studio, selecione o **nó Políticas** e clique na guia **Políticas**.
2. Clique em **Criar Política**. A lâmina **Criar Política** é aberta.
3. Procure por `Bidirectional content redirection configuration` no campo **Pesquisar**, selecione a caixa de seleção e clique em **Editar**.
4. Na lâmina **Editar Configuração**, defina esta política como **Ativada** e clique em **Gerenciar URLs**.



5. Na lâmina **Gerenciar URLs**, para **Redirecionamento VDA para cliente**, especifique o seguinte:

   - **URL** (Obrigatório): Adicione a URL que deve ser redirecionada do VDA para abrir no cliente. Para redirecionamento OAuth, defina o esquema de autenticação e o padrão no cliente para redirecionar a sessão de volta ao host.
   - **Padrão** (Opcional): Expressão regular de URL que, quando redirecionada para o cliente por meio do redirecionamento de URL VDA para Cliente, é rastreada como se um fluxo de autenticação OAuth tivesse começado, e quando o fluxo é concluído (detectado pelo esquema resultante ou padrão de URL de redirecionamento sendo aberto), essa URL resultante é redirecionada de volta para o VDA Host que iniciou esse fluxo.
   - **Esquema** (Opcional): Se um Esquema for especificado, a URL de término deverá ter o formato: `scheme://<something>`. Se o Esquema não for especificado (vazio), o padrão de URL resultante original será extraído do Padrão por meio de um grupo de captura de expressão regular (deve ser especificado no Padrão), e a URL original será reescrita para usar uma URL de redirecionamento `citrix-oauth-redir://`. Quando o fluxo é concluído, a URL de redirecionamento original é então redirecionada de volta para o Host (VDA). Qualquer servidor de autorização OAuth, neste caso, deve ser configurado para permitir URLs de redirecionamento `citrix-oauth-redir://byIndex/1 (2, 3, ... N)`.

> **Nota:**
>
> Embora **Padrão** e **Esquema** sejam opcionais, se **Padrão** for especificado, você também deve especificar **Esquema**.

6. Na lâmina **Gerenciar URLs**, para **Redirecionamento cliente para VDA**, especifique o seguinte:
   - **Tipo**: Escolha **Desktop** ou **Aplicativo**.
   - **Nome**: Forneça um nome para o tipo.
   - **URL**: Forneça a URL que você deseja redirecionar para a origem. Você pode adicionar várias URLs e excluir as que não são necessárias.
7. Clique em **Salvar**. A lâmina **Editar Configuração** exibe o número de itens configurados.
8. Clique em **Salvar**. A lâmina **Criar Política** exibe o **Valor Atual** configurado. Clique em **Avançar**.
9. Na etapa **Atribuir Política a**, clique em **Avançar**.
10. Na etapa **Resumo**, selecione a caixa de seleção **Habilitar política** e forneça um nome no campo **Nome da política**.
11. Clique em **Concluir**. A nova política é listada.
12. Selecione a nova política criada para revisar as configurações configuradas.

Para configurações legadas, consulte Redirecionamento de host para cliente e Redirecionamento de conteúdo bidirecional.

Redirecionamento do host para o cliente

> **Nota:**
>
> Este artigo descreve as configurações legadas de redirecionamento do host para o cliente. Para as configurações mais recentes, consulte Configuração de redirecionamento de conteúdo bidirecional. As novas configurações de política terão precedência sobre as configurações legadas. A Citrix recomenda usar apenas as novas configurações de política e excluir quaisquer configurações legadas para evitar comportamento inesperado.

> O redirecionamento do host para o cliente permite que URLs, incorporadas como hiperlinks em aplicativos executados em uma sessão Citrix®, sejam abertas usando o aplicativo correspondente no dispositivo de endpoint do usuário. Alguns casos de uso comuns para o redirecionamento do host para o cliente incluem:

- Redirecionamento de sites em casos em que o servidor Citrix não tem acesso à Internet ou à rede para a origem.
- Redirecionamento de sites quando a execução de um navegador da web dentro da sessão Citrix não é desejada por motivos de segurança, desempenho, compatibilidade ou escalabilidade.
- Redirecionamento de tipos de URL específicos em casos em que os aplicativos necessários para abrir a URL não estão instalados no servidor Citrix.

O redirecionamento do host para o cliente não se destina a URLs que você acessa em uma página da web ou digita na barra de endereços do navegador da web em execução na sessão Citrix. Para redirecionamento de URLs em navegadores da web, consulte Redirecionamento de URL bidirecional ou Redirecionamento de conteúdo do navegador.

Requisitos do sistema

- VDA de SO multissessão
- Clientes compatíveis:
  - Aplicativo Citrix Workspace™ para Windows
  - Aplicativo Citrix Workspace para Mac
  - Aplicativo Citrix Workspace para Linux
  - Aplicativo Citrix Workspace para HTML5
  - Aplicativo Citrix Workspace para Chrome

O dispositivo cliente deve ter um aplicativo instalado e configurado para lidar com o redirecionamento dos tipos de URL.

Configuração

Use a política Citrix de Redirecionamento do host para o cliente para habilitar essa funcionalidade. O **redirecionamento do host para o cliente** é desabilitado por padrão. Depois de habilitar a política de redirecionamento do host para o cliente, o aplicativo Citrix Launcher se registra no

servidor Windows para garantir que ele possa interceptar URLs e enviá-las para o dispositivo cliente.

Em seguida, você deve configurar a Política de Grupo do Windows para usar o Citrix Launcher como o aplicativo padrão para os tipos de URL necessários. No VDA do servidor Citrix, crie o arquivo ServerFTAdefaultPolicy.xml e insira o seguinte código XML.

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

No console de gerenciamento de Política de Grupo, vá para **Configuração do computador > Modelos Administrativos > Componentes do Windows > Explorador de Arquivos > Definir um arquivo de configuração de associações padrão**, e salve seu arquivo ServerFTAdefaultPolicy.xml.

> **Nota:**

> Se um servidor Citrix não tiver as configurações da Política de Grupo, o Windows solicitará aos usuários que selecionem um aplicativo para abrir URLs.

> Por padrão, oferecemos suporte ao redirecionamento dos seguintes tipos de URL:

- HTTP

- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

Para incluir tipos de URL padrão ou personalizados adicionais na lista para redirecionamento, crie uma nova linha **Association Identifier** no arquivo ServerFTAdefaultPolicy.xml referenciado anteriormente. Por exemplo:

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

Adicionar tipos de URL à lista também requer configuração do cliente. Crie a seguinte chave de registro e valores no cliente Windows.

> **Nota:**
>
> A edição incorreta do registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Nome do valor: ExtraURLProtocols
- Tipo de valor: REG_SZ

- Dados do valor: Especifique os tipos de URL necessários separados por ponto e vírgula. Inclua tudo antes da parte da autoridade da URL. Por exemplo: `ftp://;mailto:;customtype1://;custometype2://`

Você pode adicionar tipos de URL apenas para clientes Windows. Clientes que não possuem as configurações de registro acima rejeitam o redirecionamento de volta para a sessão Citrix. O cliente deve ter um aplicativo instalado e configurado para manipular os tipos de URL especificados.

Para remover tipos de URL da lista de redirecionamento padrão, crie a seguinte chave de registro e valores no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: DisableServerFTA
- Tipo de valor: DWORD
- Dados do valor: 1
- Nome do valor: NoRedirectClasses
- Tipo de valor: REG_MULTI_SZ
- Dados do valor: Especifique qualquer combinação dos valores: `http`, `https`, `rtsp`, `rtspu`, `pnm`, ou `mms`. Digite vários valores em linhas separadas. Por exemplo:

`http`

`https`

`rtsp`

Para habilitar o redirecionamento do host para o cliente para um conjunto específico de sites, crie uma chave de registro e valores no VDA do servidor.

- Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nome do valor: ValidSites
- Tipo de valor: REG_MULTI_SZ
- Dados do valor: Especifique qualquer combinação de nomes de domínio totalmente qualificados (FQDNs). Digite vários FQDNs em linhas separadas. Inclua apenas o FQDN, sem protocolos (`http://` ou `https://`). Um FQDN pode incluir um asterisco (`*`) como caractere curinga apenas na posição mais à esquerda. Este curinga corresponde a um único nível de domínio, o que é consistente com as regras no RFC 6125. Por exemplo:

`www.exmaple.com`

`*.example.com`

> **Nota:**
>
> Não é possível usar a chave **ValidSites** em combinação com as chaves **DisableServerFTA** e **NoRedirectClasses**.

Configuração do navegador padrão do VDA do servidor

A habilitação do redirecionamento do host para o cliente, conforme referenciado nesta seção, substitui qualquer configuração anterior do navegador padrão no VDA do servidor. Se um URL da web não for redirecionado, o Citrix Launcher passará o URL para o navegador configurado na chave de registro `command_backup`. A chave aponta para o Internet Explorer por padrão, mas você pode modificá-la para incluir o caminho para um navegador diferente. Para obter mais informações, consulte Configuração do navegador padrão do VDA do servidor na lista de recursos gerenciados por meio do registro.

Redirecionamento de conteúdo bidirecional

> **Nota:**
>
> Este artigo descreve as configurações legadas de redirecionamento de conteúdo bidirecional. Para as configurações de política mais recentes, consulte Configuração de redirecionamento de conteúdo bidirecional. As novas configurações de política terão precedência sobre as configurações legadas. A Citrix recomenda usar apenas as novas configurações de política e excluir quaisquer configurações legadas para evitar comportamentos inesperados.

> O redirecionamento de conteúdo bidirecional permite que URLs HTTP ou HTTPS em navegadores da web, ou incorporadas em aplicativos, sejam encaminhadas entre a sessão do Citrix VDA e o endpoint do cliente em ambas as direções. Uma URL inserida em um navegador em execução na sessão Citrix pode ser aberta usando o navegador padrão do cliente. Por outro lado, uma URL inserida em um navegador em execução no cliente pode

> ser aberta em uma sessão Citrix, seja com um aplicativo ou desktop publicado. Alguns casos de uso comuns para o redirecionamento de conteúdo bidirecional incluem:

- Redirecionamento de URLs da web em casos em que o navegador inicial não tem acesso à rede para a origem.
- Redirecionamento de URLs da web por motivos de compatibilidade do navegador e segurança.
- Redirecionamento de URLs da web incorporadas em aplicativos quando não se deseja executar um navegador da web na sessão Citrix ou no cliente.

Requisitos do sistema

- VDAs de SO de sessão única ou multi-sessão
- Citrix Workspace™ app para Windows

Navegadores:

- Google Chrome com a Extensão de Redirecionamento de Navegador Citrix (disponível na Google Chrome Web Store)
- Microsoft Edge (Chromium) com a Extensão de Redirecionamento de Navegador Citrix (disponível na Google Chrome Web Store)

Configuração

O redirecionamento de conteúdo bidirecional deve ser habilitado usando a política Citrix tanto no VDA quanto no cliente para que o redirecionamento funcione. O redirecionamento de conteúdo bidirecional é desabilitado por padrão.

Para a configuração do VDA, consulte Redirecionamento de conteúdo bidirecional nas configurações da política ICA.

Para a configuração do cliente, consulte Redirecionamento de conteúdo bidirecional na documentação do aplicativo Citrix Workspace para Windows.

As extensões do navegador devem ser registradas usando os comandos mostrados. Execute os comandos conforme necessário no VDA e no cliente, com base no navegador em uso.

Para registrar as extensões do navegador no VDA, abra um prompt de comando. Em seguida, execute `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` com a opção de navegador necessária, conforme mostrado nos exemplos:

`%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE`

`%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome`

`%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge`

Para registrar a extensão em todos os navegadores disponíveis, execute:

`%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall`

Para cancelar o registro de uma extensão de navegador, use a opção `/unreg<browser>` conforme mostrado no exemplo:

`%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE`

Para registrar as extensões do navegador no cliente, abra um prompt de comando e execute `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` com as mesmas opções dos exemplos mostrados.

> **Nota:**
>
> O comando de registro faz com que os navegadores Chrome e Edge solicitem aos usuários que habilitem a Extensão de Redirecionamento de Navegador Citrix durante o primeiro lançamento. A extensão do navegador também pode ser instalada manualmente na Google Chrome Web Store.

Redirecionamento curinga do Citrix VDA para o cliente

O redirecionamento de conteúdo bidirecional oferece suporte ao uso de curingas ao definir as URLs a serem redirecionadas. Para configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de configuração.

No Citrix Studio, defina a URL curinga em **Allowed URLs to be redirected to Client**. O asterisco (*) é o caractere curinga.

> **NOTA:**

- Não defina as **Allowed URLs to be redirected to VDA** na política do cliente. Certifique-se de que os sites definam as **Allowed URLs to be redirected to VDA** para evitar loops de redirecionamento infinitos.
- Domínios de nível superior não são suportados. Por exemplo, `https://www.citrix.*` ou `http://www.citrix.co*` não é redirecionado.

Redirecionamento de protocolo personalizado do VDA para o cliente

O redirecionamento de conteúdo bidirecional oferece suporte ao redirecionamento de protocolos personalizados do Citrix VDA para o cliente. Protocolos diferentes de HTTP ou HTTPS são suportados. Para configurar o redirecionamento de conteúdo bidirecional, consulte as instruções de configuração.

No Citrix Studio, defina o protocolo personalizado em **Allowed URLs to be redirected to Client**.

NOTA:

- O cliente deve ter um aplicativo registrado para manipular o protocolo. Caso contrário, a URL redireciona para o cliente e falha ao iniciar.
- URLs de protocolo personalizado que você insere ou inicia nos navegadores Chrome e Edge não são suportadas e não são redirecionadas.
- Os seguintes protocolos não são suportados: `rtsp://, rtspu://, pnm://, mms://`.

Outras considerações

- Os requisitos e configurações do navegador são aplicáveis apenas ao navegador que inicia o redirecionamento. O navegador de destino, onde a URL é aberta após o redirecionamento ser bem-sucedido, não é considerado para suporte. Ao redirecionar URLs do VDA para um cliente, uma configuração de navegador suportada é necessária apenas no VDA. Por outro lado, ao redirecionar URLs do cliente para um VDA, uma configuração de navegador suportada é necessária apenas no cliente. As URLs redirecionadas são entregues ao navegador padrão configurado na máquina de destino, seja o cliente ou o VDA, dependendo da direção. O uso do mesmo tipo de navegador no VDA e no cliente NÃO é obrigatório.

- Verifique se as regras de redirecionamento não resultam em uma configuração em loop. Por exemplo, uma política de VDA é definida para redirecionar `https://www.citrix.com`, e a política do cliente é definida para redirecionar a mesma URL, resultando em um loop infinito.
- Apenas URLs de protocolo HTTP/HTTPS são suportadas. Encurtadores de URL não são suportados.
- O redirecionamento de cliente para VDA requer que o cliente Windows seja instalado com direitos de administrador.
- Se o navegador de destino já estiver aberto, a URL redirecionada é aberta em uma nova guia. Caso contrário, a URL é aberta em uma nova janela do navegador.
- O redirecionamento bidirecional de conteúdo não funciona quando o Acesso a Aplicativos Locais (LAA) está ativado.

Acesso a aplicativos locais e redirecionamento de URL

Introdução

O Acesso a Aplicativos Locais integra perfeitamente aplicativos Windows instalados localmente em um ambiente de área de trabalho hospedada sem alternar de uma área de trabalho para outra. Com o Acesso a Aplicativos Locais, você pode:

- Acessar aplicativos instalados localmente em um laptop físico, PC ou outro dispositivo diretamente da área de trabalho virtual.
- Fornecer uma solução flexível de entrega de aplicativos. Se os usuários tiverem aplicativos locais que você não pode virtualizar ou que a TI não mantém, esses aplicativos ainda se comportarão como se estivessem instalados em uma área de trabalho virtual.
- Eliminar a latência de salto duplo quando os aplicativos são hospedados separadamente da área de trabalho virtual. Faça isso colocando um atalho para o aplicativo publicado no dispositivo Windows do usuário.
- Usar aplicativos como:
    - Software de videoconferência, como o GoToMeeting.
    - Aplicativos especializados ou de nicho que ainda não foram virtualizados.
    - Aplicativos e periféricos que, de outra forma, transfeririam grandes quantidades de dados de um dispositivo de usuário para um servidor e de volta para o dispositivo de usuário. Por exemplo, gravadores de DVD e sintonizadores de TV.

No Citrix Virtual Apps and Desktops™, as sessões de área de trabalho hospedada usam o redirecionamento de URL para iniciar aplicativos de Acesso a Aplicativos Locais. O redirecionamento de URL torna o aplicativo disponível em mais de um endereço URL. Ele inicia um navegador local (com base na lista de bloqueio de URL do navegador) selecionando links incorporados em um navegador em uma sessão de área de trabalho. Se você navegar para um URL que não está presente na lista de bloqueio, o URL será aberto novamente na sessão da área de trabalho.

O redirecionamento de URL funciona apenas para sessões de área de trabalho, não para sessões de aplicativo. O único recurso de redirecionamento que você pode usar para sessões de aplicativo é o redirecionamento de conteúdo host-para-cliente, que é um tipo de redirecionamento FTA (Associação de Tipo de Arquivo) do servidor. Este FTA redireciona certos protocolos para o cliente, como HTTP, HTTPS, RTSP ou MMS. Por exemplo, se você abrir apenas links incorporados com HTTP, os links serão abertos diretamente com o aplicativo cliente. Não há suporte para lista de bloqueio ou lista de permissões de URL.

Quando o Acesso a Aplicativos Locais está ativado, os URLs exibidos aos usuários como links de aplicativos em execução localmente, de aplicativos hospedados pelo usuário ou como atalhos na área de trabalho são redirecionados de uma das seguintes maneiras:

- Do computador do usuário para a área de trabalho hospedada
- Do servidor Citrix Virtual Apps and Desktops para o computador do usuário
- Renderizado no ambiente em que são iniciados (não redirecionados)

Para especificar o caminho de redirecionamento de conteúdo de sites específicos, configure a lista de permissões de URL e a lista de bloqueios de URL no Virtual Delivery Agent. Essas listas contêm chaves de registro de várias strings que especificam as configurações da política de redirecionamento de URL. Para obter mais informações, consulte as configurações da política de Acesso a Aplicativos Locais.

As URLs podem ser renderizadas no VDA com as seguintes exceções:

- Informações de Geo/Localidade — Sites que exigem informações de localidade, como msn.com ou news.google.com (abre uma página específica do país com base na Geo). Por exemplo, se o VDA for provisionado de um data center no Reino Unido e o cliente estiver se conectando da Índia, o usuário espera ver in.msn.com. Em vez disso, o usuário vê uk.msn.com.
- Conteúdo multimídia — Sites que contêm conteúdo de mídia rica, quando renderizados no dispositivo cliente, proporcionam aos usuários finais uma experiência nativa e também

economizam largura de banda, mesmo em redes de alta latência. Esse recurso redireciona sites com outros tipos de mídia, como Silverlight. Esse processo ocorre em um ambiente seguro. Ou seja, as URLs que o administrador aprova são executadas no cliente, enquanto o restante das URLs é redirecionado para o VDA.

Além do redirecionamento de URL, você pode usar o redirecionamento FTA. O FTA inicia aplicativos locais quando um arquivo é encontrado na sessão. Se o aplicativo local for iniciado, ele deverá ter acesso ao arquivo para abri-lo. Portanto, você só pode abrir arquivos que residem em compartilhamentos de rede ou em unidades de cliente (usando o mapeamento de unidade de cliente) usando aplicativos locais. Por exemplo, ao abrir um arquivo PDF, se um leitor de PDF for um aplicativo local, o arquivo será aberto usando esse leitor de PDF. Como o aplicativo local pode acessar o arquivo diretamente, não há transferência de rede do arquivo via ICA® para abri-lo.

Requisitos, considerações e limitações

Oferecemos suporte ao Acesso a Aplicativos Locais nos sistemas operacionais válidos para VDAs para Windows Multi-session OS e para VDAs para Windows Single-session OS. O Acesso a Aplicativos Locais requer o aplicativo Citrix Workspace para Windows versão 4.1 (mínimo). Os seguintes navegadores são suportados:

- Edge, versão mais recente
- Firefox, versão mais recente e versão de suporte estendido
- Chrome, versão mais recente

Revise as seguintes considerações e limitações ao usar o Acesso a Aplicativos Locais e o redirecionamento de URL.

- O Acesso a Aplicativos Locais foi projetado para desktops virtuais em tela cheia, abrangendo todos os monitores:
  - A experiência do usuário pode ser confusa se você usar o Acesso a Aplicativos Locais com um desktop virtual que é executado no modo de janela ou não cobre todos os monitores.
  - Vários monitores — Quando um monitor é maximizado, ele se torna o desktop padrão para todos os aplicativos iniciados nessa sessão. Esse padrão ocorre mesmo que os aplicativos subsequentes normalmente iniciem em outro monitor.
  - O recurso suporta um VDA. Não há integração com múltiplos VDAs simultâneos.
- Alguns aplicativos podem se comportar de forma inesperada, afetando os usuários:

  - As letras das unidades podem confundir os usuários, como C: local em vez da unidade C: da área de trabalho virtual.
  - As impressoras disponíveis na área de trabalho virtual não estão disponíveis para aplicativos locais.
  - Aplicativos que exigem permissões elevadas não podem ser iniciados como aplicativos hospedados no cliente.
  - Não há tratamento especial para aplicativos de instância única (como o Windows Media Player).
  - Aplicativos locais aparecem com o tema do Windows da máquina local.
  - Aplicativos em tela cheia não são suportados. Esses aplicativos incluem aplicativos que abrem em tela cheia, como apresentações de slides do PowerPoint ou visualizadores de fotos que cobrem a área de trabalho inteira.
  - O Acesso a Aplicativos Locais copia as propriedades do aplicativo local (como os atalhos na área de trabalho do cliente e no menu Iniciar) no VDA. No entanto, ele não copia outras propriedades, como teclas de atalho e atributos somente leitura.
  - Aplicativos que personalizam como a ordem das janelas sobrepostas é tratada podem ter resultados imprevisíveis. Por exemplo, algumas janelas podem ficar ocultas.
  - Atalhos não são suportados, incluindo Meu Computador, Lixeira, Painel de Controle, atalhos de Unidade de Rede e atalhos de pasta.
  - Os seguintes tipos de arquivo e arquivos não são suportados: tipos de arquivo personalizados, arquivos sem programas associados, arquivos zip e arquivos ocultos.
  - O agrupamento da barra de tarefas não é suportado para aplicativos hospedados no cliente ou VDA mistos de 32 bits e 64 bits. Ou seja, agrupar aplicativos locais de 32 bits com aplicativos VDA de 64 bits.
  - Aplicativos não podem ser iniciados usando COM. Por exemplo, se você clicar em um documento do Office incorporado de dentro de um aplicativo do Office, o início do processo não poderá ser detectado e a integração do aplicativo local falhará.

- Cenários de salto duplo, onde um usuário está iniciando uma área de trabalho virtual de dentro de outra sessão de área de trabalho virtual, não são suportados.
- O redirecionamento de URL suporta apenas URLs explícitas (ou seja, URLs que aparecem na barra de endereços do navegador ou encontradas usando a navegação no navegador, dependendo do navegador).

- O redirecionamento de URL funciona apenas com sessões de desktop, não com sessões de aplicativo.
- A pasta de desktop local em uma sessão VDA não permite que os usuários criem arquivos.
- Várias instâncias de um aplicativo em execução localmente se comportam de acordo com as configurações da barra de tarefas estabelecidas para o desktop virtual. No entanto, os atalhos para aplicativos em execução localmente não são agrupados com instâncias em execução desses aplicativos. Eles também não são agrupados com instâncias em execução de aplicativos hospedados ou atalhos fixados para aplicativos hospedados. Os usuários podem fechar apenas janelas de aplicativos em execução localmente a partir da Barra de Tarefas. Embora os usuários possam fixar janelas de aplicativos locais na Barra de Tarefas e no menu Iniciar do desktop, os aplicativos podem não iniciar de forma consistente ao usar esses atalhos.
- Se você definir a configuração de política **Permitir acesso a aplicativos locais** como **Ativado**, o redirecionamento de conteúdo do navegador não será suportado.

Interação com o Windows

A interação do Acesso a Aplicativos Locais com o Windows inclui os seguintes comportamentos.

- Comportamento de atalho do Windows 8 e Windows Server 2012
  - Os aplicativos da Windows Store instalados no cliente não são enumerados como parte dos atalhos do Acesso a Aplicativos Locais.
  - Arquivos de imagem e vídeo são abertos por padrão usando aplicativos da Windows Store. No entanto, o Acesso a Aplicativos Locais enumera os aplicativos da Windows Store e abre atalhos com aplicativos de desktop.
- Programas Locais
  - Para o Windows 7, a pasta está disponível no menu Iniciar.
  - Para o Windows 8, Programas Locais está disponível apenas quando o usuário escolhe **Todos os Aplicativos** como uma categoria na tela Iniciar. Nem todas as subpastas são exibidas em Programas Locais.
- Recursos gráficos do Windows 8 para aplicativos
  - Os aplicativos de desktop são restritos à área de trabalho e são cobertos pela tela Iniciar e aplicativos estilo Windows 8.

  - Os aplicativos de Acesso a Aplicativos Locais não se comportam como aplicativos de desktop no modo de vários monitores. No modo de vários monitores, a tela Iniciar e a área de trabalho são exibidas em monitores diferentes.

- Windows 8 e Redirecionamento de URL de Acesso a Aplicativos Locais

  - Como o Internet Explorer do Windows 8 não tem complementos habilitados, use o Internet Explorer da área de trabalho para habilitar o redirecionamento de URL.
  - No Windows Server 2012, o Internet Explorer desabilita os complementos por padrão. Para implementar o Redirecionamento de URL, desabilite a configuração aprimorada do Internet Explorer. Em seguida, redefina as opções do Internet Explorer e reinicie para garantir que os complementos estejam habilitados para usuários padrão.

Configurar Acesso a Aplicativos Locais e redirecionamento de URL

Para usar o Acesso a Aplicativos Locais e o redirecionamento de URL com o aplicativo Citrix Workspace™:

- Instale o aplicativo Citrix Workspace na máquina cliente local. Você pode habilitar os dois recursos durante a instalação do aplicativo Citrix Workspace ou pode habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo.
- Defina a configuração da política **Permitir acesso a aplicativos locais** como **Habilitado**. Você também pode configurar as configurações de política de lista de permissões e lista de bloqueios de URL para redirecionamento de URL. Para obter mais informações, consulte Configurações de política de Acesso a Aplicativos Locais.

Habilitar Acesso a Aplicativos Locais e redirecionamento de URL

Para habilitar o Acesso a Aplicativos Locais para todos os aplicativos locais, siga estas etapas:

1. No Studio, selecione **Políticas** no painel esquerdo.
2. Selecione **Criar Política** na barra de ações.
3. Na janela Criar Política, digite “Permitir Acesso a Aplicativos Locais” na caixa de pesquisa e clique em **Selecionar**.
4. Na janela Editar Configuração, selecione **Permitido**. Por padrão, a política **Permitir acesso a aplicativos locais** é proibida. Quando essa configuração é permitida, o VDA permite que o usuário final decida se os aplicativos publicados e os atalhos de Acesso a Aplicativos Locais são habilitados na sessão. (Quando essa configuração é proibida, tanto os aplicativos publicados quanto os atalhos de Acesso a Aplicativos Locais não funcionam para o VDA.)

Essa configuração de política se aplica a toda a máquina e à política de redirecionamento de URL.

5. Na janela Criar Política, digite “lista de permissões de redirecionamento de URL” na caixa de pesquisa e clique em **Selecionar**. A lista de permissões de redirecionamento de URL especifica as URLs a serem abertas no navegador padrão da sessão remota.
6. Na janela Editar Configuração, clique em **Adicionar** para adicionar os URLs e, em seguida, clique em **OK**.
7. Na janela Criar Política, digite “lista de bloqueio de redirecionamento de URL” na caixa de pesquisa e, em seguida, clique em **Selecionar**. A lista de bloqueio de redirecionamento de URL especifica os URLs que são redirecionados para o navegador padrão em execução no endpoint.
8. Na janela Editar Configuração, clique em **Adicionar** para adicionar os URLs e, em seguida, clique em **OK**.
9. Na página Configurações, clique em **Avançar**.
10. Na página Usuários e Máquinas, atribua a política aos Grupos de Entrega aplicáveis e, em seguida, clique em **Avançar**.
11. Na página Resumo, revise as configurações e, em seguida, clique em **Concluir**.

Para habilitar o redirecionamento de URL para todos os aplicativos locais durante a instalação do aplicativo Citrix Workspace, siga as etapas abaixo:

1. Habilite o redirecionamento de URL ao instalar o aplicativo Citrix Workspace para todos os usuários em uma máquina. Isso também registra os complementos do navegador necessários para o redirecionamento de URL.
2. No prompt de comando, execute o comando apropriado para instalar o aplicativo Citrix Workspace usando uma das seguintes opções:
   - Para CitrixReceiver.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
   - Para CitrixReceiverWeb.exe, use `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

Habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo

> **Nota:**

- Antes de habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo, adicione os arquivos de modelo `receiver.admx/adml` ao GPO local. Para obter mais informações, consulte Introdução e pesquise por *modelo administrativo de Objeto de Política de Grupo*.
- Os arquivos de modelo do aplicativo Citrix Workspace para Windows estão disponíveis no GPO local na pasta **Modelos Administrativos > Componentes Citrix > Citrix Workspace** somente quando você adiciona o `CitrixBase.admx/CitrixBse.adml` à pasta %systemroot%\policyDefinitions.

Para habilitar o modelo de Acesso a Aplicativos Locais usando o editor de Política de Grupo, siga estas etapas:

1. Execute **gpedit.msc**.
2. Vá para **Configuração do Computador > Modelos Administrativos > Modelos Administrativos Clássicos (ADM) > Componentes Citrix > Citrix Workspace > Experiência do Usuário**.
3. Clique em **Configurações de Acesso a Aplicativos Locais**.
4. Selecione **Habilitado** e, em seguida, selecione **Permitir Redirecionamento de URL**. Para redirecionamento de URL, registre os complementos do navegador usando a linha de comando descrita na seção *Registrar complementos do navegador* mais adiante neste artigo.

Fornecer acesso apenas a aplicativos publicados

Você pode fornecer acesso a aplicativos publicados usando o Editor do Registro ou o SDK do PowerShell.

Para o Editor do Registro, consulte O Acesso a Aplicativos Locais para aplicativos publicados na lista de recursos gerenciados através do registro.

Para usar o SDK do PowerShell:

1. Abra o PowerShell na máquina onde o Delivery Controller™ está sendo executado.
2. Insira o seguinte comando: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`.

Para ter acesso a **Adicionar Aplicativo de Acesso a Aplicativos Locais** em uma implantação do Citrix DaaS, use o SDK Remoto do PowerShell do Citrix Virtual Apps and Desktops. Para mais informações, consulte SDK Remoto do PowerShell do Citrix Virtual Apps and Desktops.

1. Baixe o instalador:

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`

2. Execute estes comandos:

   a. `asnp citrix.*`.

   b. `Get-XdAuthentication`

3. Insira o seguinte comando: `set-configsitemetadata -name “studio_clientHostedAppsEnabled” -value “true”`.

Depois de concluir as etapas anteriores aplicáveis, siga estas etapas para continuar.

1. No Studio, selecione **Applications** no painel esquerdo.
2. No painel superior central, clique com o botão direito do mouse na área em branco e selecione **Add Local App Access Application** no menu. Você também pode clicar em **Add Local App Access Application** no painel Ações. Para exibir a opção Add Local App Access Application no painel Ações, clique em **Refresh**.
3. Publique o aplicativo Local App Access.

   - O assistente de Acesso a Aplicativos Locais é iniciado com uma página de Introdução, que você pode remover de futuras inicializações do assistente.
   - O assistente o guiará pelas páginas Grupos, Localização, Identificação, Entrega e Resumo, descritas abaixo. Ao terminar cada página, clique em **Next** até chegar à página Resumo.
   - Na página Grupos, selecione um ou mais Delivery Groups onde os novos aplicativos serão adicionados e, em seguida, clique em **Next**.
   - Na página Localização, digite o caminho executável completo do aplicativo na máquina local do usuário e digite o caminho para a pasta onde o aplicativo está localizado. A Citrix recomenda que você use o caminho da variável de ambiente do sistema; por exemplo, %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.
   - Na página Identificação, aceite os valores padrão ou digite as informações desejadas e, em seguida, clique em **Next**.
   - Na página Entrega, configure como este aplicativo é entregue aos usuários e, em seguida, clique em **Next**. Você pode especificar o ícone para o aplicativo selecionado. Você também pode especificar se o atalho para o aplicativo local na área de trabalho virtual será visível no menu Iniciar, na área de trabalho ou em ambos.

- Na página Resumo, revise as configurações e, em seguida, clique em **Finish** para sair do assistente de Acesso a Aplicativos Locais.

Registrar complementos do navegador

> **Nota:**
>
> Os complementos do navegador necessários para o redirecionamento de URL são registrados automaticamente ao instalar o aplicativo Citrix Workspace a partir da linha de comando usando a opção `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
>
> Você pode usar os seguintes comandos para registrar e cancelar o registro de um ou todos os complementos:

- Para registrar complementos em um dispositivo cliente: \<*pasta-de-instalação-do-cliente*>\redirector.exe /reg\<*navegador*>
- Para cancelar o registro de complementos em um dispositivo cliente: \<*pasta-de-instalação-do-cliente*>\redirector.exe /unreg\<*navegador*>
- Para registrar complementos em um VDA: \<*pasta-de-instalação-do-VDA*>\VDARedirector.exe /reg\<*navegador*>
- Para cancelar o registro de complementos em um VDA: \<*pasta-de-instalação-do-VDA*>\VDARedirector.exe /unreg\<*navegador*>

Onde \<*navegador*> é Internet Explorer, Firefox, Chrome ou Todos.

Por exemplo, o seguinte comando registra complementos do Internet Explorer em um dispositivo que executa o aplicativo Citrix Workspace.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

O seguinte comando registra todos os complementos em um VDA de SO multissessão do Windows.

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

Intercepção de URL entre navegadores

- Por padrão, o Internet Explorer redireciona a URL especificada. Se a URL não estiver na lista de bloqueio, mas o navegador ou site a redirecionar para outra URL, a URL final não será redirecionada. Ela não é redirecionada mesmo que esteja na lista de bloqueio.

Para que o redirecionamento de URL funcione corretamente, habilite o complemento quando solicitado pelo navegador. Se os complementos que usam as opções da Internet ou os complementos no prompt estiverem desabilitados, o redirecionamento de URL não funcionará corretamente.

- Os complementos do Firefox sempre redirecionam as URLs.

Quando um complemento é instalado, o Firefox solicita que você permita ou impeça a instalação do complemento em uma nova página de guia. Permita o complemento para que o recurso funcione.

- O complemento do Chrome sempre redireciona a URL final para a qual se navega, e não as URLs inseridas.

As extensões foram instaladas externamente. Quando você desativa a extensão, o recurso de redirecionamento de URL não funciona no Chrome. Se o redirecionamento de URL for necessário no modo de navegação anônima, permita que a extensão seja executada nesse modo nas configurações do navegador.

Configurar o comportamento do aplicativo local ao fazer logoff e desconectar

> **Nota:**

> Se você não seguir estas etapas para configurar as definições, por padrão, os aplicativos locais continuarão a ser executados quando um usuário fizer logoff ou se desconectar da área de trabalho virtual. Após a reconexão, os aplicativos locais são reintegrados se estiverem disponíveis na área de trabalho virtual.

> Para configurar o comportamento do aplicativo local ao fazer logoff e desconectar, consulte Comportamento do aplicativo local ao fazer logoff e desconectar na lista de recursos gerenciados por meio do registro.

Redirecionamento USB genérico e considerações sobre unidades de cliente

A tecnologia HDX™ oferece **suporte otimizado** para a maioria dos dispositivos USB populares. O suporte otimizado oferece uma experiência de usuário aprimorada com melhor desempenho e eficiência de largura de banda em uma WAN. O suporte otimizado geralmente é a melhor opção, especialmente em ambientes de alta latência ou sensíveis à segurança.

A tecnologia HDX oferece **redirecionamento USB genérico** para dispositivos especializados que não possuem suporte otimizado ou onde ele é inadequado, por exemplo:

- O dispositivo USB possui recursos mais avançados que não fazem parte do suporte otimizado, como um mouse ou webcam com mais botões.
- Os usuários precisam de funções que não fazem parte do suporte otimizado.
- O dispositivo USB é um dispositivo especializado, como equipamento de teste e medição ou um controlador industrial.
- Um aplicativo requer acesso direto ao dispositivo como um dispositivo USB.
- O dispositivo USB tem apenas um driver Windows disponível. Por exemplo, um leitor de cartão inteligente pode não ter um driver disponível para o aplicativo Citrix Workspace™ para Android.
- A versão do aplicativo Citrix Workspace não oferece suporte otimizado para este tipo de dispositivo USB.

Com o redirecionamento USB genérico:

- Os usuários não precisam instalar drivers de dispositivo no dispositivo do usuário.
- Os drivers de cliente USB são instalados na máquina VDA.

Importante:

- O redirecionamento USB genérico pode ser usado em conjunto com o suporte otimizado. Se você habilitar o redirecionamento USB genérico, configure as configurações de política de dispositivos USB do Citrix para redirecionamento USB genérico e suporte otimizado.
- A configuração de política do Citrix em Regras de otimização de dispositivo USB do cliente é uma configuração específica para redirecionamento USB genérico, para um

dispositivo USB específico. Ela não se aplica ao suporte otimizado conforme descrito aqui.

- Ao intermediar uma sessão usando o software Citrix® para uma Máquina Virtual do Azure, a Citrix oferece suporte de melhor esforço para o redirecionamento USB para a Máquina Virtual do Azure. Oferecemos suporte para corrigir um problema de software Citrix, mas não oferecemos suporte à Máquina Virtual do Azure subjacente.
- Dispositivos de CD/DVD com recursos de gravação de disco podem ser redirecionados, mas os recursos de gravação desses dispositivos não podem ser usados. Isso se deve aos limites de buffer de uma sessão.

Considerações de desempenho para dispositivos USB

A latência da rede e a largura de banda podem afetar a experiência do usuário e a operação do dispositivo USB ao usar o redirecionamento USB genérico para alguns tipos de dispositivos USB. Por exemplo, dispositivos sensíveis ao tempo podem não funcionar corretamente em links de alta latência e baixa largura de banda. Use o suporte otimizado sempre que possível.

Alguns dispositivos USB exigem alta largura de banda para serem utilizáveis, por exemplo, um mouse 3D (usado com aplicativos 3D que também geralmente exigem alta largura de banda). Se a largura de banda não puder ser aumentada, você poderá mitigar o problema ajustando o uso da largura de banda de outros componentes usando as configurações da política de largura de banda. Para obter mais informações, consulte Configurações da política de largura de banda para redirecionamento de dispositivo USB do cliente e Configurações da política de conexão multi-stream.

Considerações de segurança para dispositivos USB

Alguns dispositivos USB são sensíveis à segurança por natureza, por exemplo, leitores de cartão inteligente, leitores de impressão digital e mesas digitalizadoras de assinatura. Outros dispositivos USB, como dispositivos de armazenamento USB, podem ser usados para transmitir dados que podem ser confidenciais.

Dispositivos USB são frequentemente usados para distribuir malware. A configuração do Citrix Workspace app e do Citrix Virtual Apps and Desktops™ pode reduzir, mas não eliminar, o risco desses dispositivos USB. Essa situação se aplica independentemente de ser usado o redirecionamento USB genérico ou o suporte otimizado.

Importante:

Para dispositivos e dados sensíveis à segurança, sempre proteja a conexão HDX usando TLS ou IPsec.

Habilite o suporte apenas para os dispositivos USB de que você precisa. Configure o redirecionamento USB genérico e o suporte otimizado para atender a essa necessidade.

Forneça orientação aos usuários para o uso seguro de dispositivos USB:

- Use apenas dispositivos USB obtidos de uma fonte confiável.
- Não deixe dispositivos USB sem vigilância em ambientes abertos - por exemplo, um pen drive em um cybercafé.
- Explique os riscos de usar um dispositivo USB em mais de um computador.

Compatibilidade com redirecionamento USB genérico

O redirecionamento USB genérico é compatível com dispositivos USB 2.0 e anteriores. O redirecionamento USB genérico também é compatível com dispositivos USB 3.0 conectados a uma porta USB 2.0 ou USB 3.0. O redirecionamento USB genérico não oferece suporte a recursos USB introduzidos no USB 3.0, como super velocidade.

Estes aplicativos Citrix Workspace oferecem suporte ao redirecionamento USB genérico:

- Aplicativo Citrix Workspace para Windows, consulte Configurando a entrega de aplicativos.
- Aplicativo Citrix Workspace para Mac, consulte Citrix Workspace app for Mac.
- Aplicativo Citrix Workspace para Linux, consulte Otimizar.
- Aplicativo Citrix Workspace para Chrome OS, consulte Citrix Workspace app for Chrome.

Para versões do aplicativo Citrix Workspace, consulte a matriz de recursos do aplicativo Citrix Workspace.

Se você estiver usando versões anteriores do aplicativo Citrix Workspace, consulte a documentação do aplicativo Citrix Workspace para confirmar se o redirecionamento USB genérico é compatível. Consulte a documentação do aplicativo Citrix Workspace para quaisquer restrições sobre os tipos de dispositivos USB compatíveis.

O redirecionamento USB genérico é compatível com sessões de desktop do VDA para SO de sessão única, versão 7.6 até a atual.

O redirecionamento USB genérico é compatível com sessões de desktop do VDA para SO de múltiplas sessões, versão 7.6 até a atual, com estas restrições:

- O VDA deve estar executando Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 ou Windows Server 2022.
- Os drivers de dispositivo USB devem ser totalmente compatíveis com o Host de Sessão da Área de Trabalho Remota (RDSH) para o SO do VDA (Windows 2012 R2), incluindo suporte total à virtualização.

Alguns tipos de dispositivos USB não são compatíveis com o redirecionamento USB genérico porque não seria útil redirecioná-los:

- Modems USB.
- Adaptadores de rede USB.
- Hubs USB. Os dispositivos USB conectados a hubs USB são tratados individualmente.
- Portas COM virtuais USB. Use o redirecionamento de porta COM em vez do redirecionamento USB genérico.

Para obter informações sobre dispositivos USB que foram testados com o redirecionamento USB genérico, consulte Citrix Ready Marketplace. Alguns dispositivos USB não funcionam corretamente com o redirecionamento USB genérico.

Configurar o redirecionamento USB genérico

Você pode controlar e configurar separadamente quais tipos de dispositivos USB usam o redirecionamento USB genérico:

- No VDA, usando as configurações de política do Citrix. Para obter mais informações, consulte Redirecionamento de unidades de cliente e dispositivos de usuário e Configurações de política de dispositivos USB na referência de configurações de política.
- No aplicativo Citrix Workspace, usando mecanismos dependentes do aplicativo Citrix Workspace. Por exemplo, um Modelo Administrativo controla as configurações de registro que configuram o aplicativo Citrix Workspace para Windows. Por padrão, o redirecionamento USB é permitido para certas classes de dispositivos USB e negado para outras. Para obter mais informações, consulte Configurar na documentação do aplicativo Citrix Workspace para Windows.

Essa configuração separada oferece flexibilidade. Por exemplo:

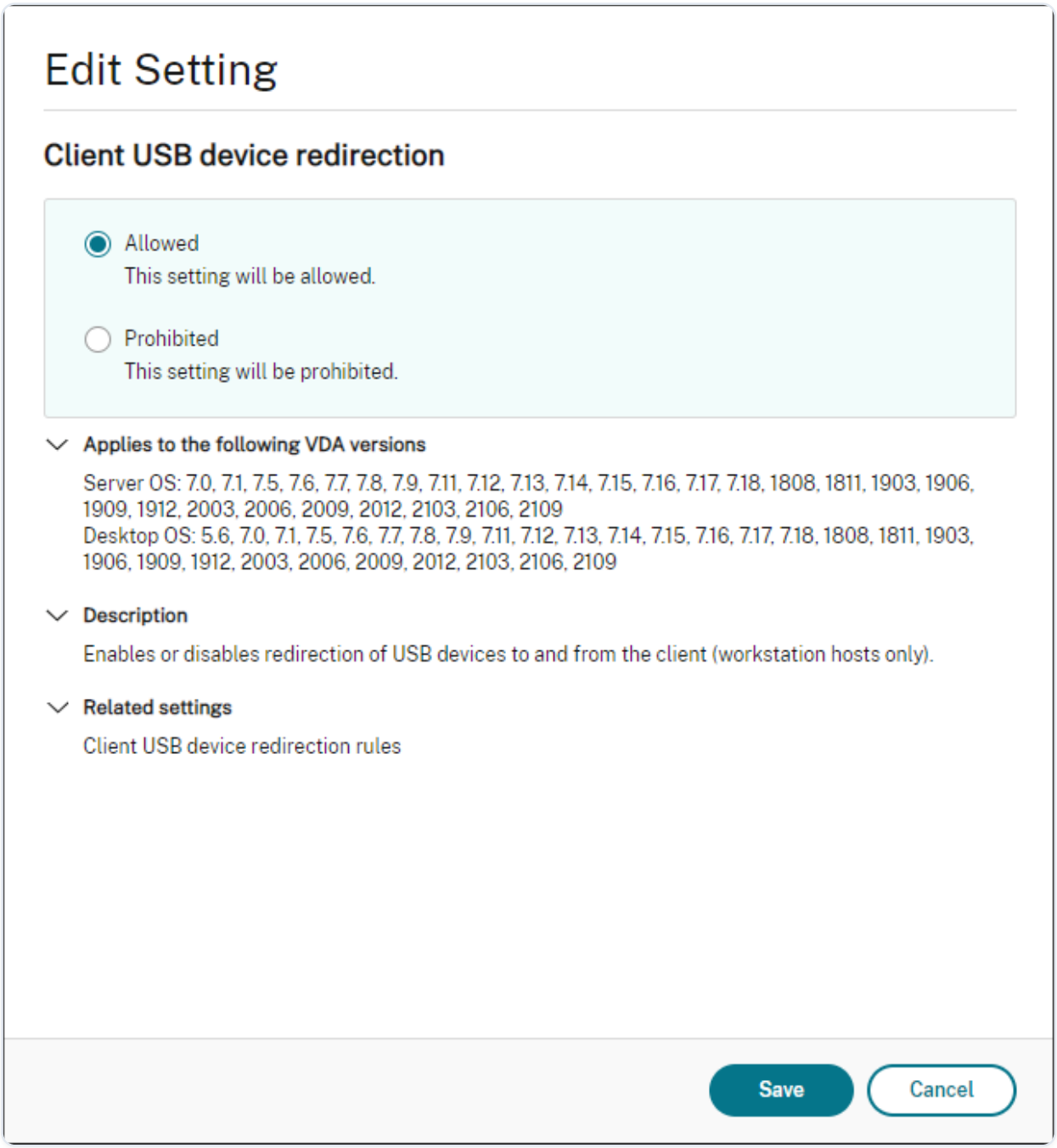
- Se duas organizações ou departamentos diferentes forem responsáveis pelo aplicativo Citrix Workspace e pelo VDA, eles poderão impor o controle separadamente. Essa configuração se aplica quando um usuário em uma organização acessa um aplicativo em outra organização.
- As configurações de política do Citrix podem controlar dispositivos USB que são permitidos apenas para determinados usuários ou para usuários que se conectam apenas por uma LAN (em vez de usar o Citrix Gateway).

Habilitar o redirecionamento USB genérico

Para habilitar o redirecionamento USB genérico e não exigir o redirecionamento manual pelo usuário, configure as configurações de política do Citrix e as preferências de conexão do aplicativo Citrix Workspace.

Nas configurações de política do Citrix:

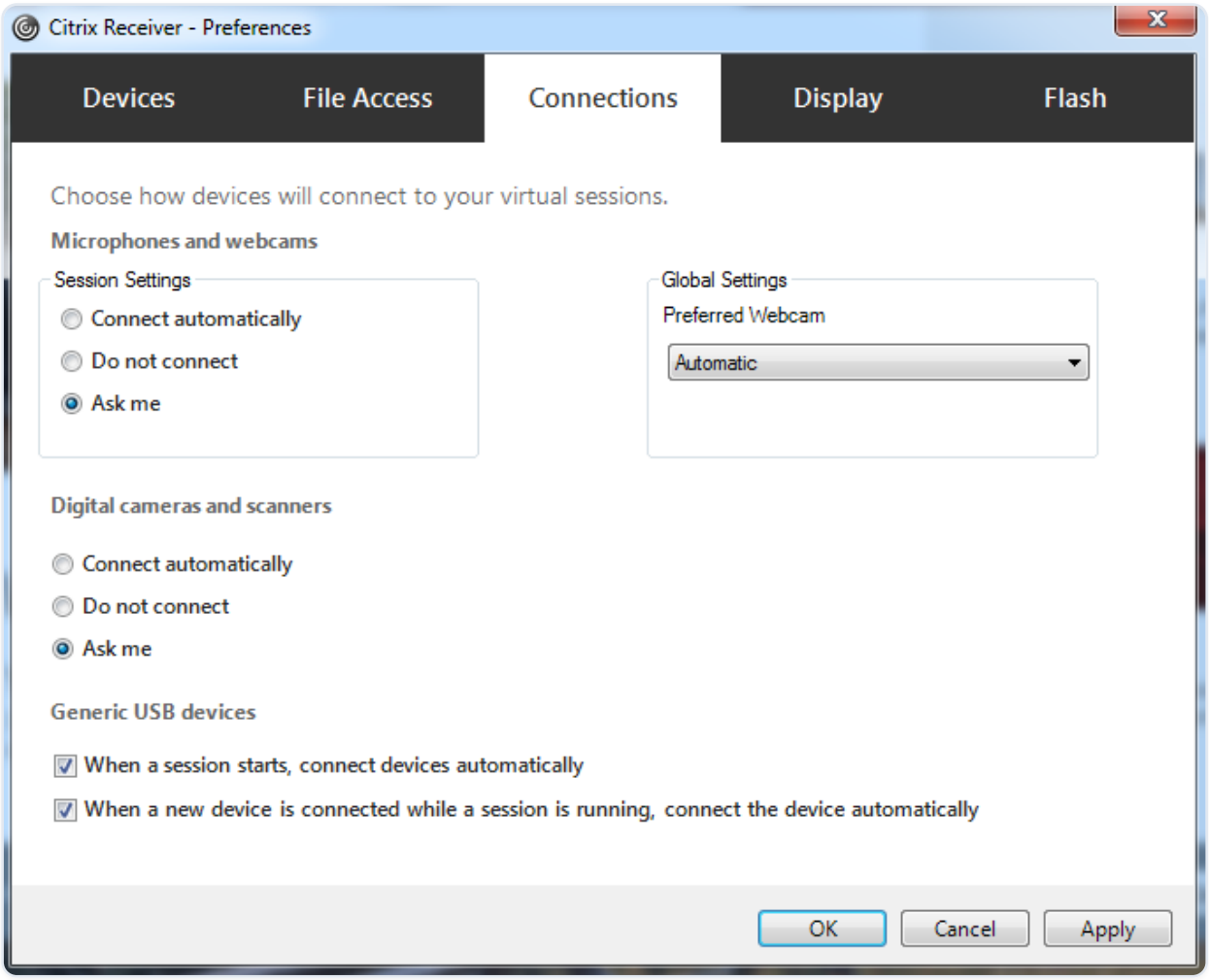
1. Adicione o Redirecionamento de dispositivo USB do cliente a uma política e defina seu valor como **Permitido**.



2. (Opcional) Para atualizar a lista de dispositivos USB disponíveis para redirecionamento, adicione a configuração Regras de redirecionamento de dispositivo USB do cliente a uma política e especifique as regras de política USB.

   No aplicativo Citrix Workspace:

3. Especifique que os dispositivos sejam conectados automaticamente sem redirecionamento manual. Você pode fazer isso usando um modelo administrativo ou no aplicativo Citrix Workspace para Windows > Preferências > Conexões.



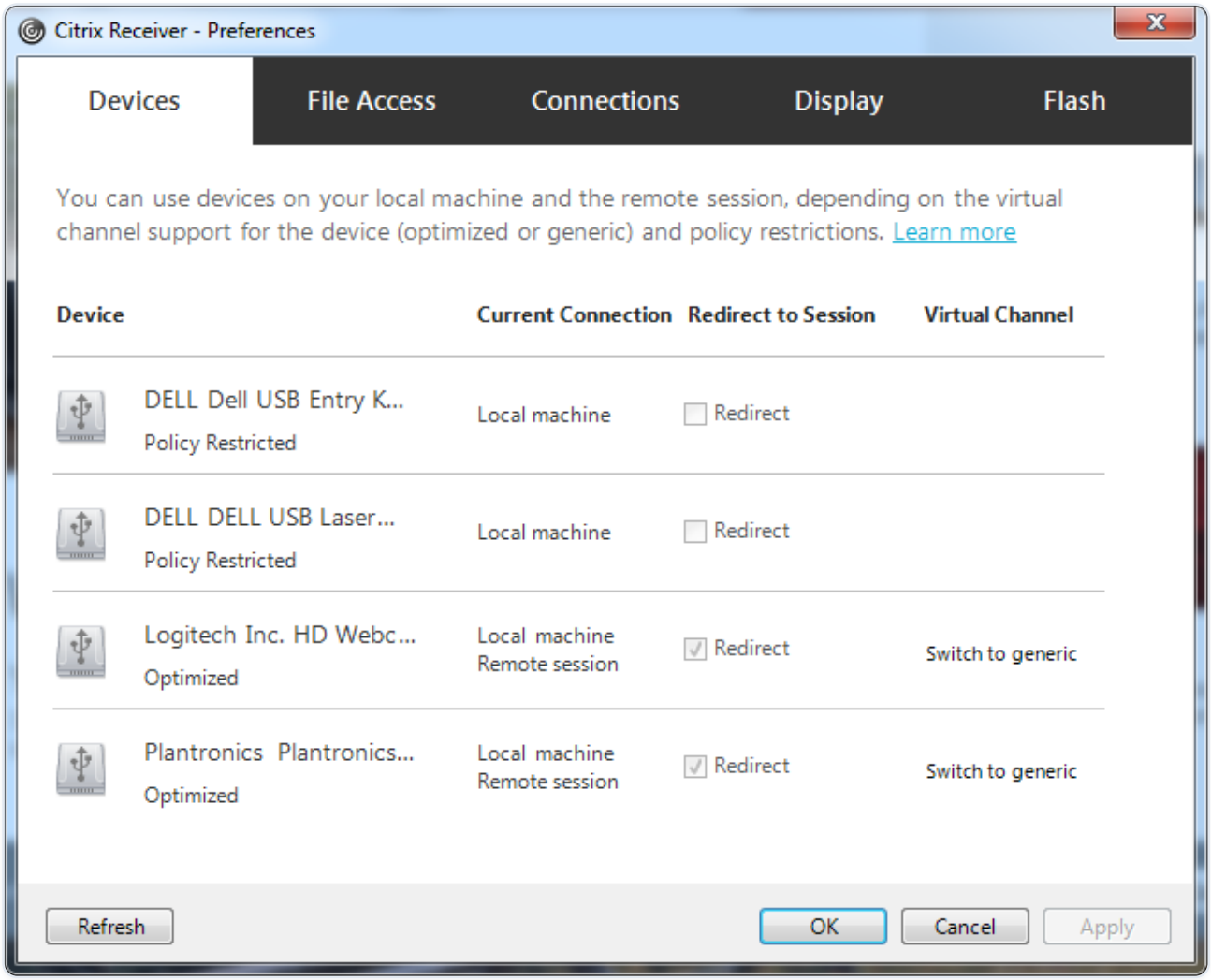
Se você especificou regras de política USB para o VDA na etapa anterior, especifique as mesmas regras de política para o aplicativo Citrix Workspace.

Para thin clients, consulte o fabricante para obter detalhes sobre o suporte USB e qualquer configuração necessária.

Configurando os tipos de dispositivos USB disponíveis para redirecionamento USB genérico

Os dispositivos USB são redirecionados automaticamente quando o suporte USB está ativado e as configurações de preferência do usuário USB estão definidas para conectar dispositivos USB automaticamente. Os dispositivos USB também são redirecionados automaticamente quando a barra de conexão não está presente.

Os usuários podem redirecionar explicitamente dispositivos que não são redirecionados automaticamente, selecionando os dispositivos na lista de dispositivos USB. Para obter mais informações, consulte o artigo de ajuda do usuário do aplicativo Citrix Workspace para Windows, Exibir seus dispositivos no Desktop Viewer.



Para usar o redirecionamento USB genérico em vez do suporte otimizado, você pode:

- No aplicativo Citrix Workspace, selecione manualmente o dispositivo USB para usar o redirecionamento USB genérico, escolha **Mudar para genérico** na guia Dispositivos da caixa de diálogo Preferências.
- Selecione automaticamente o dispositivo USB para usar o redirecionamento USB genérico, configurando o redirecionamento automático para o tipo de dispositivo USB (por exemplo, AutoRedirectStorage=1) e defina as configurações de preferência do usuário USB para conectar dispositivos USB automaticamente. Para obter mais informações, consulte Configurar o redirecionamento automático de dispositivos USB.

> **Nota:**
>
> Configure a redireção USB genérica para uso com uma webcam apenas se a webcam for considerada incompatível com a redireção multimídia HDX.

> Para evitar que dispositivos USB sejam listados ou redirecionados, você pode especificar regras de dispositivo para o aplicativo Citrix Workspace e o VDA.

Para a redireção USB genérica, você precisa saber pelo menos a classe e a subclasse do dispositivo USB. Nem todos os dispositivos USB usam sua classe e subclasse de dispositivo USB óbvias. Por exemplo:

- Canetas usam a classe de dispositivo de mouse.
- Leitores de cartão inteligente podem usar a classe de dispositivo definida pelo fornecedor ou HID.

Para um controle mais preciso, você precisa saber o ID do Fornecedor, o ID do Produto e o ID da Versão. Você pode obter essas informações do fornecedor do dispositivo.

> **Importante:**

> Dispositivos USB maliciosos podem apresentar características de dispositivo USB que não correspondem ao seu uso pretendido. As regras de dispositivo não se destinam a impedir esse comportamento.

> Você controla os dispositivos USB disponíveis para redireção USB genérica especificando regras de redireção de dispositivo USB para o VDA e o aplicativo Citrix Workspace, para substituir as regras de política USB padrão.

Para o VDA:

- Edite as regras de substituição do administrador para as máquinas do SO de várias sessões por meio de regras de política de grupo. O Console de Gerenciamento de Política de Grupo está incluído na mídia de instalação:
  - Para x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Para x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

No aplicativo Citrix Workspace para Windows:

- Edite o registro do dispositivo do usuário. Um modelo administrativo (arquivo ADM) está incluído na mídia de instalação para que você possa alterar o dispositivo do usuário por meio da Política de Grupo do Active Directory: dvd root \os\lang\Support\Configuration\icaclient_usb.adm

Aviso:

A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

As regras padrão do produto são armazenadas em HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. Não edite essas regras padrão do produto. Em vez disso, use-as como um guia para criar regras de substituição do administrador, o que é explicado mais adiante neste artigo. As substituições de GPO são avaliadas antes das regras padrão do produto.

As regras de substituição do administrador são armazenadas em HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. As regras de política de GPO seguem o formato **{Allow:`|`Deny:}** seguido por um conjunto de expressões *tag=value* separadas por espaço em branco.

As seguintes tags são suportadas:

TAG	DESCRIÇÃO
VID	ID do Fornecedor do descritor do dispositivo
PID	ID do Produto do descritor do dispositivo
REL	ID de Lançamento do descritor do dispositivo
Classe	Classe do descritor do dispositivo ou de um descritor de interface; consulte o site da USB em `<http://www.usb.org/>` para obter os Códigos de Classe USB disponíveis
SubClasse	Subclasse do descritor do dispositivo ou de um descritor de interface
Prot	Protocolo do descritor do dispositivo ou de um descritor de interface

Ao criar regras de política, observe o seguinte:

- As regras não diferenciam maiúsculas de minúsculas.
- As regras podem ter um comentário opcional no final, introduzido por `#`. Um delimitador não é necessário, e o comentário é ignorado para fins de correspondência.
- Linhas em branco e linhas de comentário puro são ignoradas.
- Espaços em branco são usados como separadores, mas não podem aparecer no meio de um número ou identificador. Por exemplo, Deny: Class = 08 SubClass=05 é uma regra válida, mas Deny: Class=0 Sub Class=05 não é.
- As tags devem usar o operador de correspondência =. Por exemplo, VID=1230.
- Cada regra deve começar em uma nova linha ou fazer parte de uma lista separada por ponto e vírgula.

> **Nota:**
>
> Se você estiver usando o arquivo de modelo ADM, deverá criar regras em uma única linha, como uma lista separada por ponto e vírgula.

> Exemplos:

- O exemplo a seguir mostra uma regra de política USB definida pelo administrador para identificadores de fornecedor e produto:

  `Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products`

- O exemplo a seguir mostra uma regra de política USB definida pelo administrador para uma classe, subclasse e protocolo definidos:

  `Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices`

Usar e remover dispositivos USB

Os usuários podem conectar um dispositivo USB antes ou depois de iniciar uma sessão virtual.

Ao usar o aplicativo Citrix Workspace para Windows, o seguinte se aplica:

- Os dispositivos conectados após o início de uma sessão aparecem imediatamente no menu USB do Desktop Viewer.
- Se um dispositivo USB não estiver sendo redirecionado corretamente, você pode tentar resolver o problema esperando para conectar o dispositivo até depois que a sessão virtual for iniciada.
- Para evitar a perda de dados, use o ícone "Remover Hardware com Segurança" do Windows antes de remover o dispositivo USB.

Controles de segurança para dispositivos de armazenamento em massa USB

O suporte otimizado é fornecido para dispositivos de armazenamento em massa USB. Esse suporte faz parte do mapeamento de unidade cliente do Citrix Virtual Apps and Desktops. As unidades no dispositivo do usuário são automaticamente mapeadas para letras de unidade na área de trabalho virtual quando os usuários fazem logon. As unidades são exibidas como pastas compartilhadas que têm letras de unidade mapeadas. Para configurar o mapeamento de unidade cliente, use a configuração **Unidades removíveis do cliente**. Essa configuração está na seção Configurações de política de redirecionamento de arquivo das configurações de política ICA.

Com dispositivos de armazenamento em massa USB, você pode usar o mapeamento de unidade cliente ou o redirecionamento USB genérico, ou ambos. Controle-os usando políticas Citrix. As principais diferenças são:

RECURSO	MAPEAMENTO DE UNIDADE CLIENTE	REDIRECIONAMENTO USB GENÉRICO
Ativado por padrão	Sim	Não
Acesso somente leitura configurável	Sim	Não
Acesso a dispositivo criptografado	Sim, se a criptografia for desbloqueada antes que o dispositivo seja acessado	Sim
Dispositivos BitLocker To Go	Não	Não
Seguro para excluir o dispositivo durante uma sessão	Não	Sim, desde que os usuários sigam as recomendações do sistema operacional para remoção segura

Se as políticas de redirecionamento USB genérico e de mapeamento de unidade cliente estiverem habilitadas e um dispositivo de armazenamento em massa for inserido antes ou depois do início de uma sessão, ele será redirecionado usando o mapeamento de unidade cliente. Quando as políticas de redirecionamento USB genérico e de mapeamento de unidade cliente estiverem habilitadas e um dispositivo for configurado para redirecionamento automático e um dispositivo de armazenamento em massa for inserido antes ou depois do início de uma sessão, ele será redirecionado usando o redirecionamento USB genérico. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX123015.

Nota:

O redirecionamento USB é suportado em conexões de menor largura de banda, por exemplo, 50 Kbps. No entanto, a cópia de arquivos grandes não funciona.

Gerenciar

A Citrix gerencia as implantações do serviço Citrix Virtual Apps and Desktops™ instalando e mantendo os componentes e recursos principais no Citrix Cloud.

Você cuida das máquinas (VDAs) nos locais de recursos que entregam aplicativos e desktops. Você também gerencia as conexões com esses locais de recursos, além dos aplicativos, desktops e usuários.

- Autoscale**:** Uma solução consistente e de alto desempenho para gerenciar proativamente a energia de suas máquinas.
- Aplicativos**:** Gerencie aplicativos em grupos de entrega.
- IP virtual e loopback virtual**:** O recurso de endereço IP virtual da Microsoft fornece a um aplicativo publicado um endereço IP exclusivo atribuído dinamicamente para cada sessão. Com o loopback virtual da Citrix, você pode configurar aplicativos que dependem de comunicações com o localhost (127.0.0.1 por padrão) para usar um endereço de loopback virtual exclusivo no intervalo do localhost (127.*).
- Registro de VDA**:** Antes que um VDA possa facilitar a entrega de aplicativos e desktops, ele deve se registrar (estabelecer comunicação) com um Cloud Connector. Você pode especificar endereços de Cloud Connector usando vários métodos, que são descritos neste artigo. À medida que você adiciona Cloud Connectors, os VDAs devem ter informações atualizadas.
- Sessões**:** Manter a atividade da sessão é fundamental para proporcionar a melhor experiência ao usuário. Vários recursos podem otimizar a confiabilidade das sessões, reduzir inconvenientes, tempo de inatividade e perda de produtividade.
- Usando a Pesquisa**:** Para visualizar informações sobre máquinas, sessões, catálogos de máquinas, aplicativos ou grupos de entrega no Studio, use o recurso de pesquisa flexível.
- Suporte a IPv4/IPv6**:** O Citrix Virtual Apps and Desktops oferece suporte a implantações puras de IPv4, puras de IPv6 e dual-stack que usam redes IPv4 e IPv6 sobrepostas. Este artigo descreve e ilustra essas implantações. Ele também descreve as configurações de política da Citrix que controlam o uso de IPv4 ou IPv6.
- Gerenciamento de perfil**:** O Citrix Profile Management pode ser instalado quando você instala um VDA. Se você usar esta solução de perfil de usuário, revise sua documentação.

- Citrix Insight Services**:** O Citrix Insight Services (CIS) é uma plataforma Citrix para instrumentação, telemetria e geração de insights de negócios. Análises e diagnósticos são coletados quando você instala um VDA.
- Cache de Host Local**:** O Cache de Host Local permite que as operações de intermediação de conexão continuem quando um Cloud Connector em um local de recurso não consegue se comunicar com o Citrix Cloud. Escala, tamanho e outras considerações de configuração também são fornecidos.
- Administração delegada**:** Com a administração delegada, você pode configurar as permissões de acesso que todos os seus administradores precisam, de acordo com sua função em sua organização.
- Registro de configuração**:** O registro de configuração rastreia as alterações de configuração e as atividades administrativas.
- Registros de eventos**:** Os serviços dentro do Citrix Virtual Apps and Desktops registram os eventos que ocorrem. Os registros de eventos podem ser usados para monitorar e solucionar problemas de operações.
- Licenças**:** Você pode visualizar as informações de uso da licença Citrix para este serviço no console do Citrix Cloud.
- Balancear carga de máquinas**:** Você pode controlar como balancear a carga das máquinas.

Acesso adaptativo

Nas situações em constante mudança de hoje, a segurança de aplicativos é vital para qualquer negócio. Tomar decisões de segurança cientes do contexto e, em seguida, habilitar o acesso aos aplicativos reduz os riscos associados, ao mesmo tempo em que permite o acesso aos usuários.

O recurso de acesso adaptativo oferece uma abordagem abrangente de acesso de confiança zero que fornece acesso seguro aos aplicativos. O acesso adaptativo permite que os administradores forneçam acesso em nível granular aos aplicativos que os usuários podem acessar com base no contexto. O termo "contexto" refere-se a:

- Usuários e grupos (usuários e grupos de usuários)
- Dispositivos (dispositivos de desktop ou móveis)
- Localização (geolocalização ou localização de rede)
- Postura do dispositivo (verificação da postura do dispositivo)
- Risco (pontuação de risco do usuário)

Serviço de Postura do Dispositivo

O serviço Citrix Device Posture é uma solução baseada em nuvem que ajuda os administradores a impor certos requisitos que os dispositivos finais devem atender para obter acesso ao Citrix DaaS (Citrix Virtual Apps™ e Desktops) ou aos recursos do Citrix Secure Private Access (aplicativos SaaS e Web ou aplicativos TCP e UDP). Estabelecer a confiança do dispositivo verificando a postura do dispositivo é fundamental para implementar o acesso baseado em confiança zero. O serviço Device Posture impõe princípios de confiança zero em sua rede, verificando a conformidade dos dispositivos finais (postura gerenciada/BYOD e de segurança) antes de permitir que um usuário final faça login.

Para obter detalhes, consulte Postura do Dispositivo.

Serviço de Autenticação Adaptativa

A Autenticação Adaptativa é um serviço Citrix Cloud™ que permite autenticação avançada para clientes e usuários que fazem login em lojas na nuvem. O serviço de Autenticação Adaptativa é um ADC gerenciado pela Citrix e hospedado no Citrix Cloud que oferece todos os recursos avançados de autenticação, como os seguintes:

- Autenticação multifator usando diferentes métodos de autenticação como AD, RADIUS, certificado, vários IdPs de terceiros usando SAML 2.0, OAuth, OIDC, Google Captcha.
- Verificar a identidade do usuário e os níveis de autorização com base em fatores como localização, status do dispositivo e grupo de usuários.
- Habilitar acesso contextual ou inteligente a DaaS (virtualizado) e SPA (recursos não virtualizados como aplicativos Web e SaaS).
- Personalização da página de login

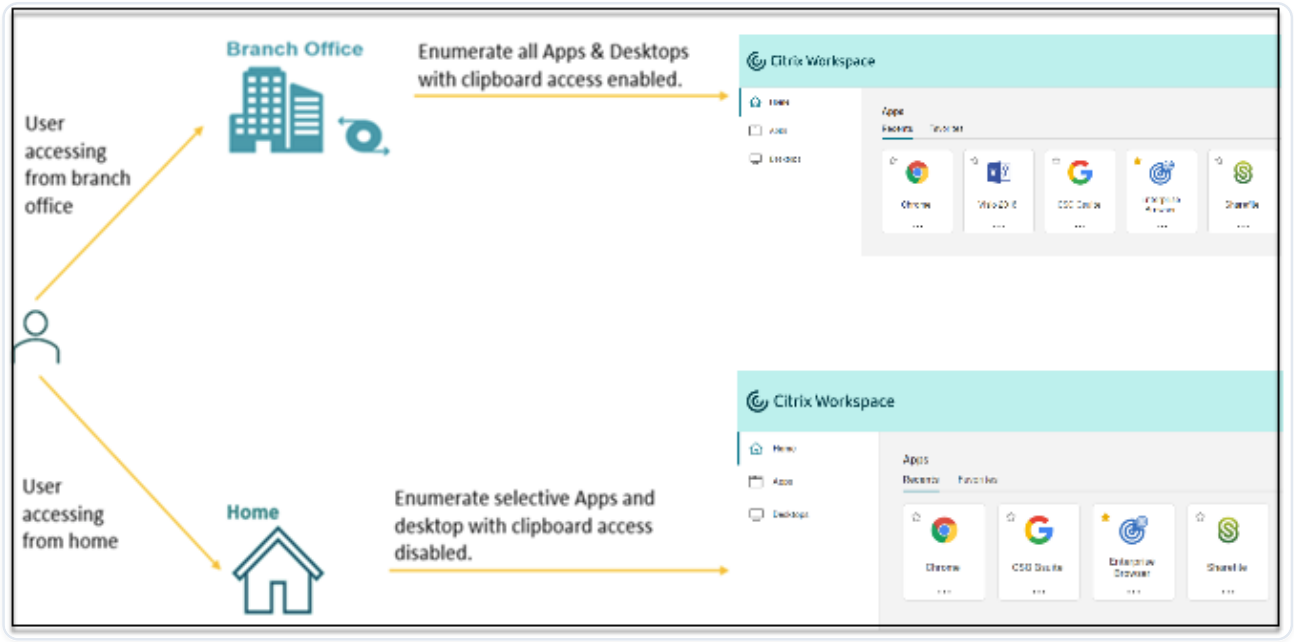
Para detalhes completos sobre Autenticação Adaptativa, consulte Serviço de Autenticação Adaptativa.

Acesso adaptativo baseado na localização de rede do usuário

O recurso de Acesso Adaptativo do Citrix® StoreFront Cloud usa uma infraestrutura de política avançada para permitir o acesso ao Citrix DaaS™ com base na localização de rede do usuário. A localização é definida usando o intervalo de endereços IP ou endereços de sub-rede.

Os administradores podem definir políticas para enumerar ou não enumerar aplicativos e desktops virtuais com base na localização de rede do usuário. Os administradores também podem controlar as ações do usuário ativando ou desativando o acesso à área de transferência, impressoras,

mapeamento de unidades de cliente e assim por diante, com base na localização de rede do usuário. Por exemplo, os administradores podem configurar políticas de forma que os usuários que acessam os recursos de casa tenham acesso limitado aos aplicativos e os usuários que acessam os recursos de filiais tenham acesso total.



Um administrador pode implementar as seguintes políticas para acessar os aplicativos:

- Enumerar alguns aplicativos sensíveis apenas a partir da localização corporativa ou de suas filiais.
- Não enumerar aplicativos sensíveis se os funcionários estiverem acessando o workspace de uma rede externa.
- Desativar o acesso à impressora a partir das filiais.
- Desativar o acesso à área de transferência e o acesso à impressora quando os usuários estiverem fora da rede corporativa.

Direitos

O recurso de Acesso Adaptativo está disponível como parte da Licença Universal Híbrida Multi Nuvem (UHMC) e da Licença de Plataforma (CPL). Para obter mais informações, consulte `<https://www.citrix.com/buy/licensing/product.html>`.

Pré-requisitos

- Certifique-se de que o recurso **Acesso Adaptativo** esteja ativado (**StoreFront Cloud > Acesso > Acesso Adaptativo**). Para obter detalhes, consulte Ativar o recurso Acesso Adaptativo.

Quando o acesso adaptativo é ativado, as políticas de acesso do DaaS são atualizadas para usar a opção **Conexões através do Citrix Gateway**.

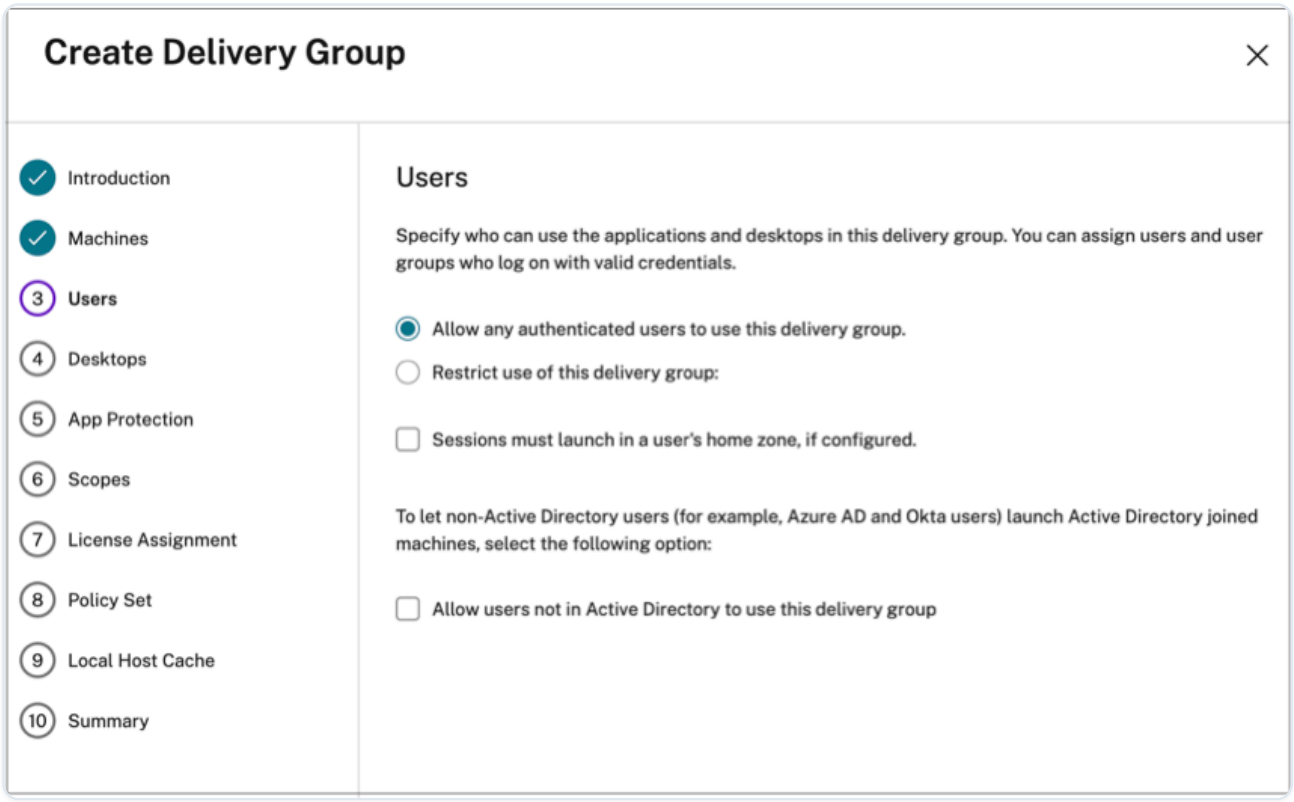
> **Nota:**
>
> O NetScaler® Gateway é necessário para adicionar tags de acesso inteligente nas políticas de acesso do DaaS. No entanto, como o DaaS consome tags dos serviços de Postura do Dispositivo, Acesso Adaptativo e Autenticação Adaptativa, não é necessário ter um NetScaler Gateway configurado em sua configuração.

- Compreensão das tags de localização. Para obter detalhes, consulte Tags de Localização de Rede.

Pontos a serem observados

Os pontos a seguir são aplicáveis apenas se você quiser restringir a enumeração de aplicativos com base na localização. Se você planeja usar o acesso adaptativo para restringir controles de usuário, como desabilitar o acesso à área de transferência, o redirecionamento de impressora, o mapeamento de unidades de cliente, com base na localização da rede, você pode ignorar estas diretrizes.

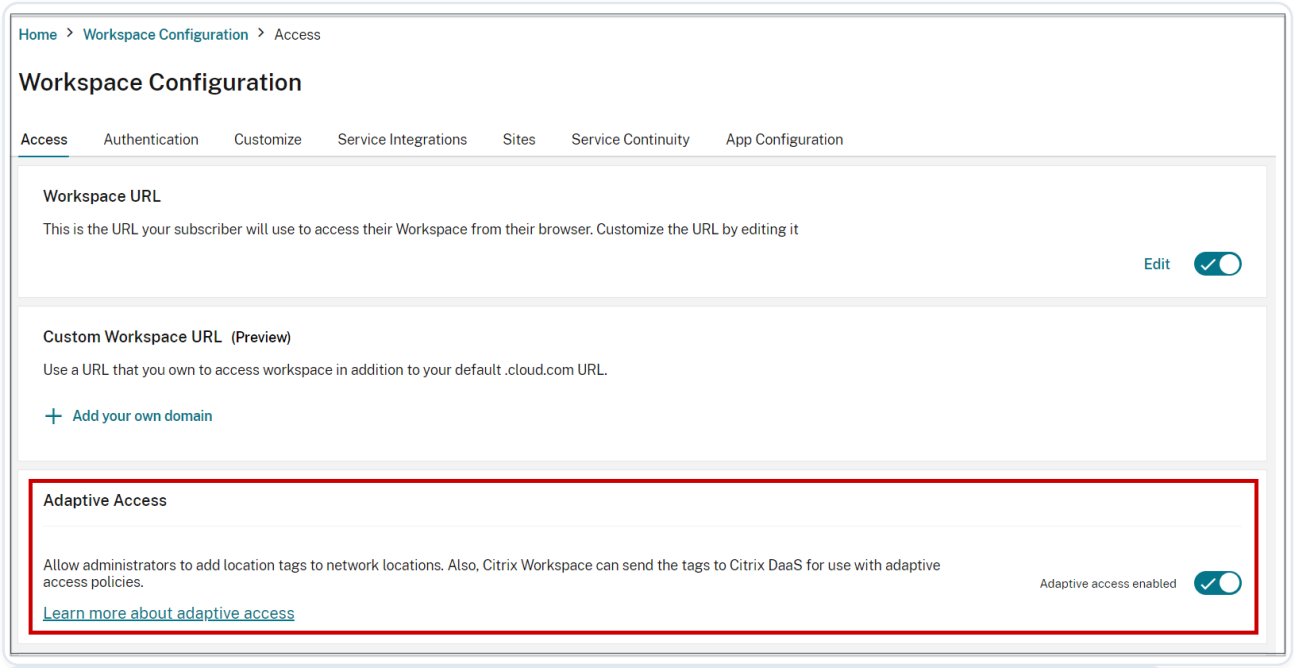
- Se você planeja enumerar seletivamente o Citrix DaaS com base na localização da rede, o gerenciamento de usuários deve ser realizado para esses grupos de entrega usando políticas do Citrix Studio em vez do workspace. Ao criar um Grupo de Entrega, em **Configuração de Usuários**, escolha **Restringir o uso deste Grupo de Entrega** para usuários ou **Permitir que qualquer usuário autenticado use este Grupo de Entrega**. Isso permite configurar o acesso adaptativo na guia **Política de Acesso** em **Grupo de Entrega**.

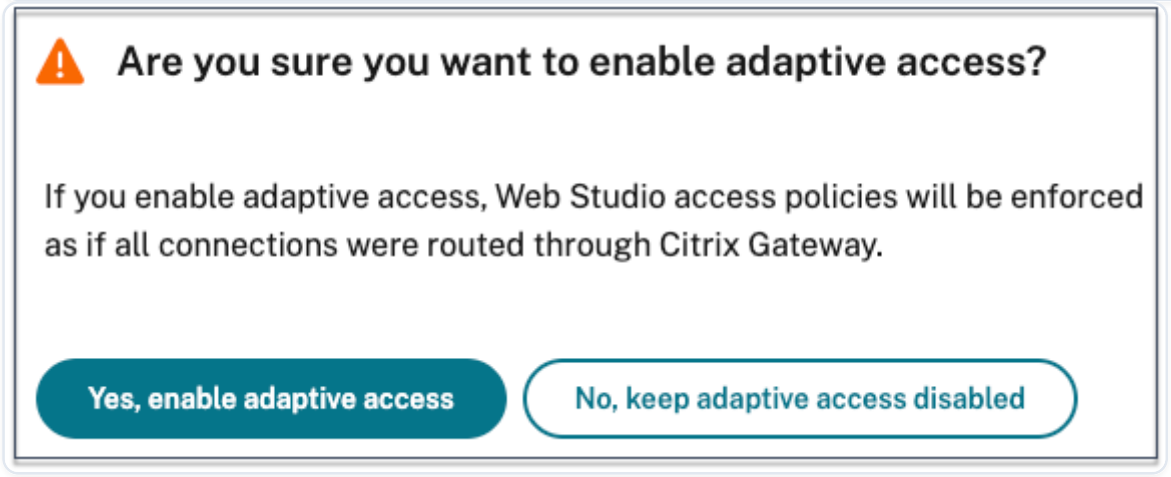


- Alterações na Conexão Direta de Carga de Trabalho quando o acesso adaptativo está habilitado.
  - O campo **Tags de localização** está visível em **Citrix Cloud™ > Locais de Rede > Adicionar um Local de Rede > Tags de localização**.
  - As políticas existentes de Conexão Direta de Carga de Trabalho funcionam conforme o esperado.
  - Novas políticas devem ser criadas no serviço Locais de Rede (sem definir tags) e também no grupo de entrega. Além disso, o tipo de conectividade de rede deve ser **Interno**.
  - Para novas políticas de Conexão Direta de Carga de Trabalho com tags, as tags devem ser definidas no serviço Locais de Rede e as mesmas tags também devem ser definidas no grupo de entrega ou na política de acesso no DaaS Studio. Além disso, o tipo de conectividade de rede deve ser **Interno**. As tags de localização não são relevantes para a Conexão Direta de Carga de Trabalho.
- O seguinte é recomendado para testar sua implantação do Citrix DaaS.
  - Identifique um grupo de entrega de teste ou crie um grupo de entrega para implementar essa capacidade.
  - Crie uma política ou identifique uma política que possa ser usada com um grupo de entrega de teste.

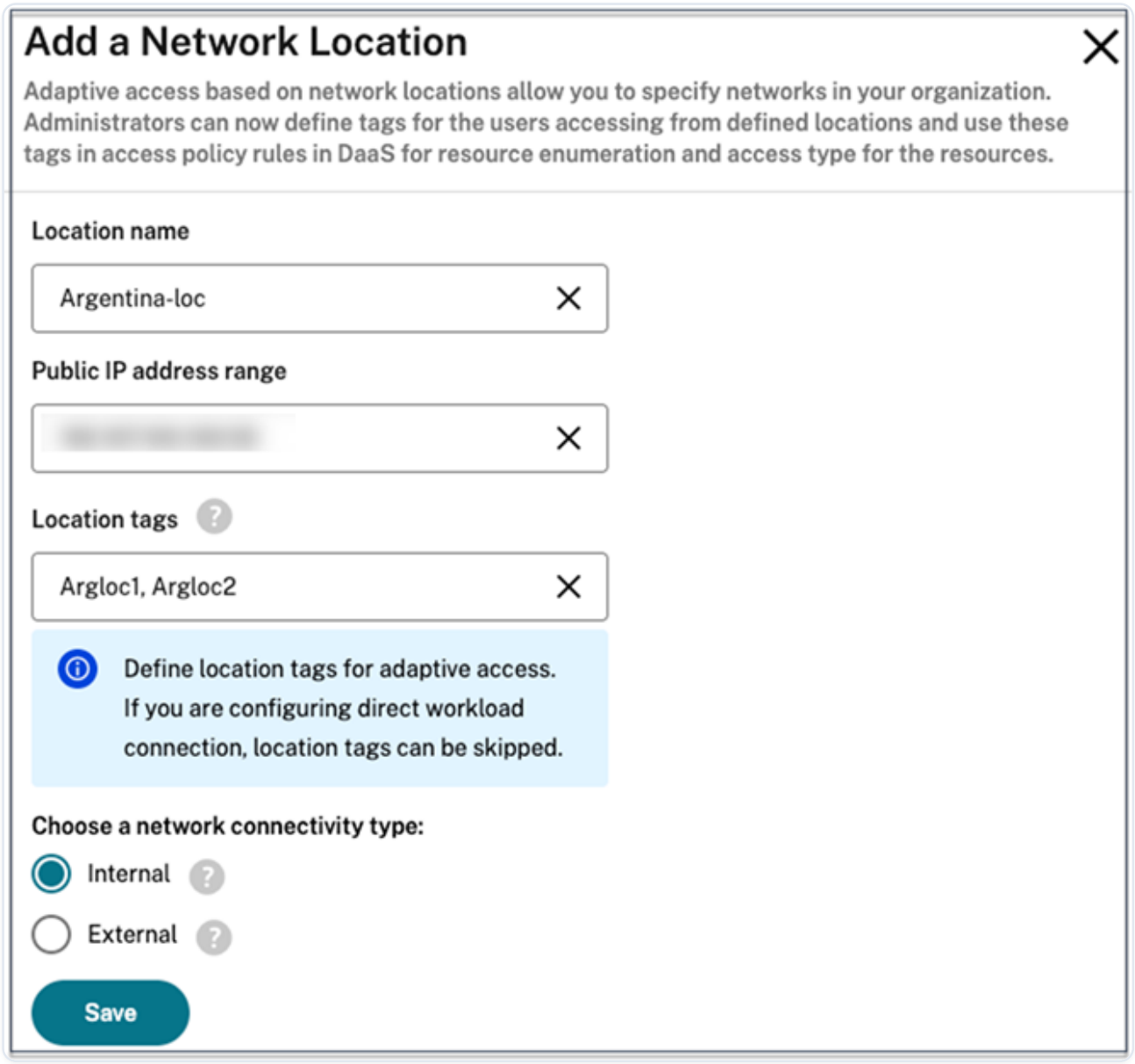
Habilitar o recurso de Acesso Adaptativo

1. Faça login no Citrix Cloud.
2. Selecione **StoreFront Cloud** no menu hambúrguer.
3. O botão de alternância **Adaptive Access** está desativado por padrão. Ative o botão de alternância **Adaptive Access**.
4. Clique em **Sim, habilitar acesso adaptativo** na mensagem de confirmação.

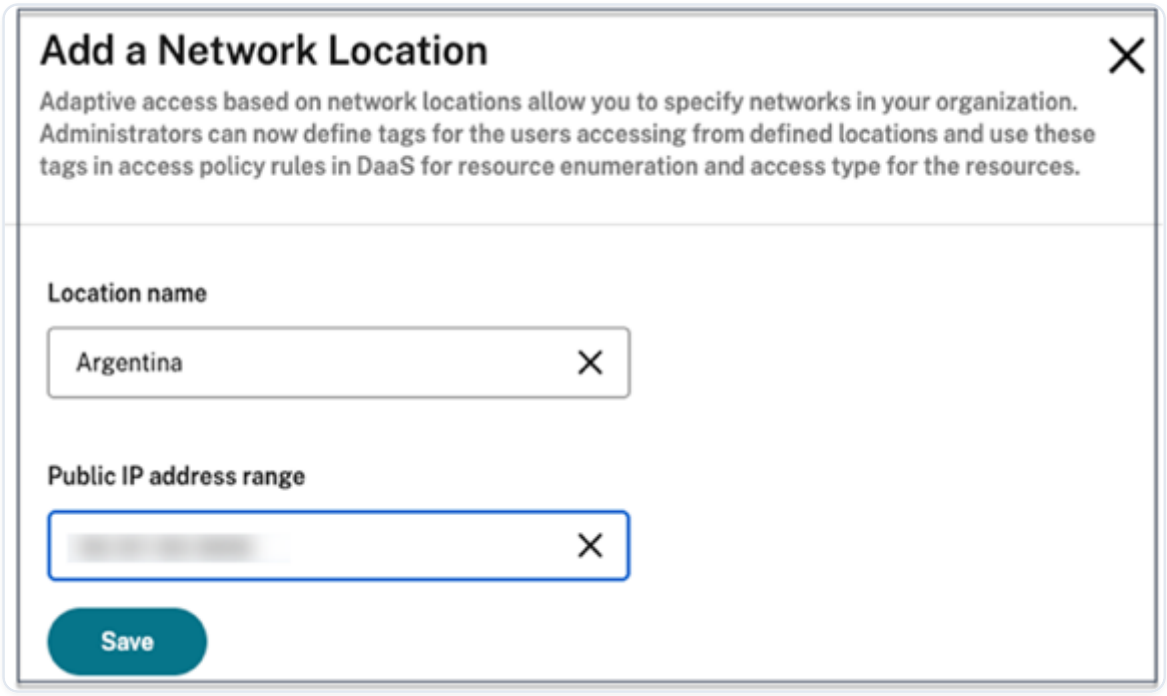




Quando o acesso adaptativo está habilitado, você pode definir as tags de localização para acesso adaptativo (**Citrix Cloud > Network Locations > Add a Network Location > Location tags**).

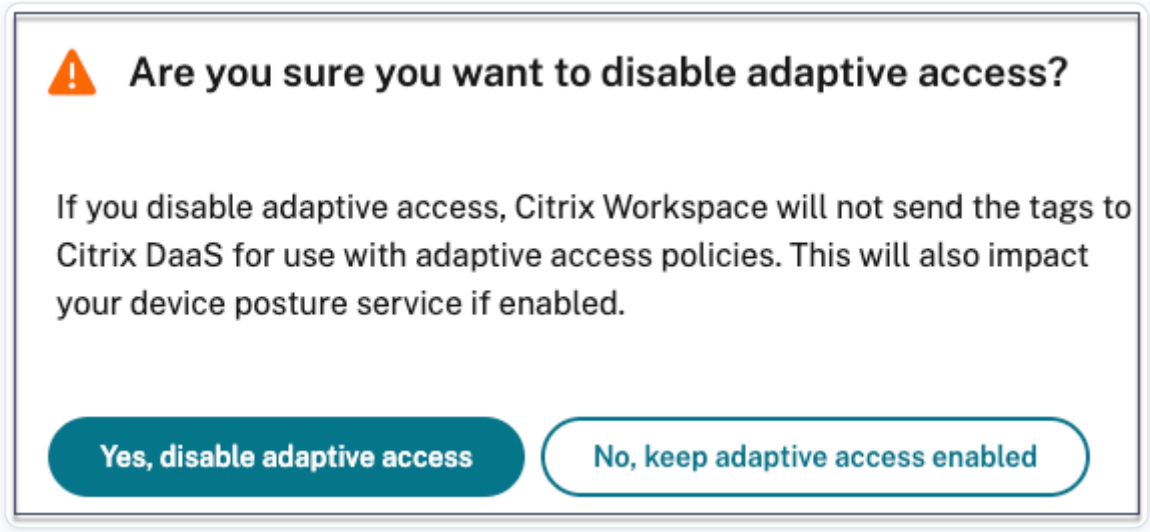


Quando o Acesso Adaptativo está desabilitado, você não pode adicionar um local de rede. As tags de localização não são aplicáveis neste caso.



Importante:

Quando você tenta desabilitar o recurso Acesso Adaptativo, a seguinte mensagem aparece. Observe que o Workspace não envia as tags para o DaaS para acesso adaptativo quando o recurso está desabilitado.



Configurar acesso adaptativo

Considere um cenário em que um administrador precisa impor o controle de acesso com base nos locais de rede dos usuários (por exemplo, escritório e casa). O administrador também deve impor controles inteligentes, como restrições de área de transferência para usuários que trabalham em

casa. Para alcançar este cenário com acesso adaptativo, o administrador deve criar 2 grupos de entrega com base na rede do usuário:

- Grupo de entrega de **Acesso Adaptativo** para BranchOffice com aplicativos relevantes para usuários de filiais.
- Grupo de entrega **WFH** para WorkFromHome com aplicativos relevantes para usuários domésticos/remotos.

Após a criação dos grupos de entrega, as seguintes etapas de alto nível estão envolvidas na configuração do acesso adaptativo com base nos locais de rede:

- Defina tags e configure as políticas de localização de rede.
- Use as tags definidas em grupos de entrega para enumeração de aplicativos e/ou aplique controles inteligentes em aplicativos.
- Aplique controles inteligentes em aplicativos (opcional).

Definir tags de localização de rede para acesso baseado em localização

A primeira etapa envolve a definição de tags para usuários com base em suas localizações; escritório ou casa.

- **BRANCHOFFICE:** Esta tag deve ser atribuída a usuários que se conectam da rede do escritório. Esses usuários têm acesso total a todos os aplicativos disponíveis para eles.
- **WORKFROMHOME:** Esta tag deve ser atribuída a usuários que trabalham remotamente. Esses usuários têm acesso limitado a aplicativos e a certos recursos (como a funcionalidade da área de transferência).

Para obter mais informações sobre tags, consulte Tags de Localização de Rede.

Agora que você tem os grupos de entrega e as tags respectivas criadas com base na localização do usuário, você pode prosseguir para a configuração da política de localização de rede.

Configurar as políticas de localização de rede

Defina regras de política de localização de rede para a localização do seu usuário, fornecendo o endereço IP de origem público e a tag de localização.

1. Faça login no Citrix Cloud.
2. Selecione **Locais de Rede** no menu hambúrguer. Certifique-se de que o botão de alternância Acesso Adaptativo esteja ativado. Caso contrário, a interface do usuário para a Conexão Direta de Carga de Trabalho será exibida.

3. Clique em **Adicionar local de rede**.

   - **Nome do local:** Insira um nome apropriado para a política.

     Exemplo: BRANCHOFFICE ou WORKFROMHOME

   - **Intervalo de endereço IP público:** Defina o intervalo de endereço IP público para sua rede.

     Exemplo: 192.0.2.10 - 192.0.2.30

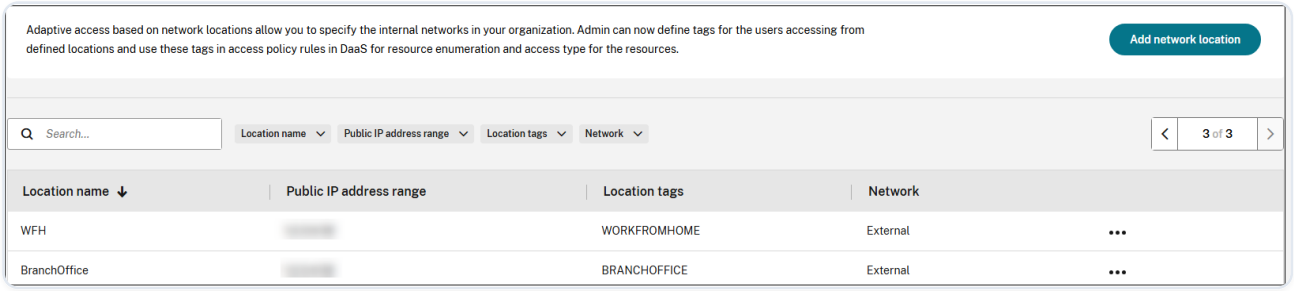
   - **Tags de Localização:** Defina tags para sua localização. Pode ser um nome que se refere à sua localização. Essas tags são usadas para configurar as políticas de acesso adaptativo no Citrix Studio. Para obter detalhes, consulte **Definir tags no Citrix Studio**.

     Exemplo: BRANCHOFFICE ou WORKFROMHOME

   - **Tipo de conectividade:** Defina o tipo de inicialização do aplicativo.

   Interno - Ignorar gateway para inicialização de aplicativo. **Externo** - Usar o serviço Citrix Gateway ou gateway tradicional para inicialização de aplicativo.

4. Clique em **Salvar**.



Agora você pode usar essas tags no DaaS Studio para habilitar o acesso adaptativo.

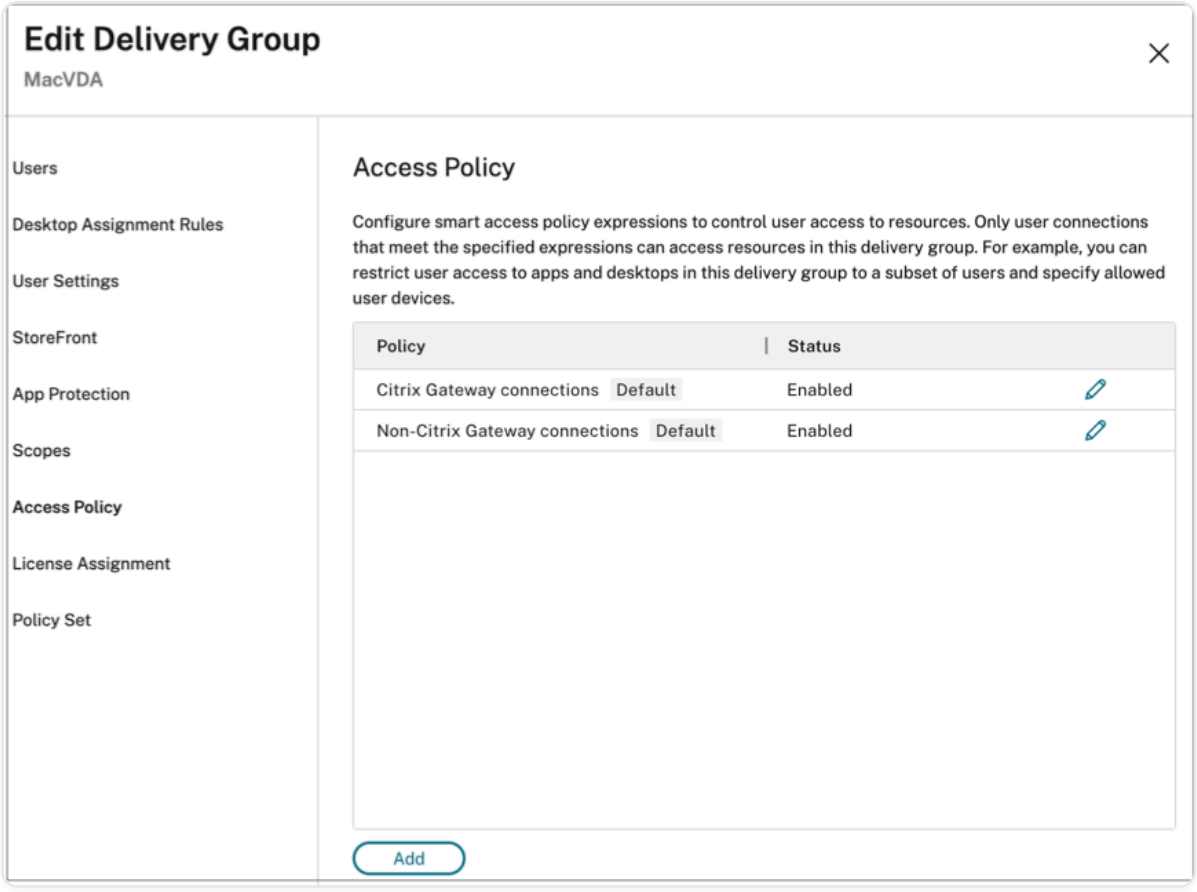
Nota:

- Se as tags de local de rede não forem atribuídas aos grupos de entrega, os usuários recebem acesso irrestrito a todos os aplicativos nos grupos de entrega de Acesso Adaptativo e WFH. Isso pode resultar em cenários em que os usuários podem acessar inadvertidamente certos aplicativos para os quais não estão autorizados. A atribuição de tags de localização aos grupos de entrega garante que o acesso seja controlado com base na localização de rede dos usuários.
- Ao definir as tags de localização, certifique-se de inserir apenas o nome da tag preferencial sem o prefixo “LOCATION_TAG”, por exemplo BRANCHOFFICE. No

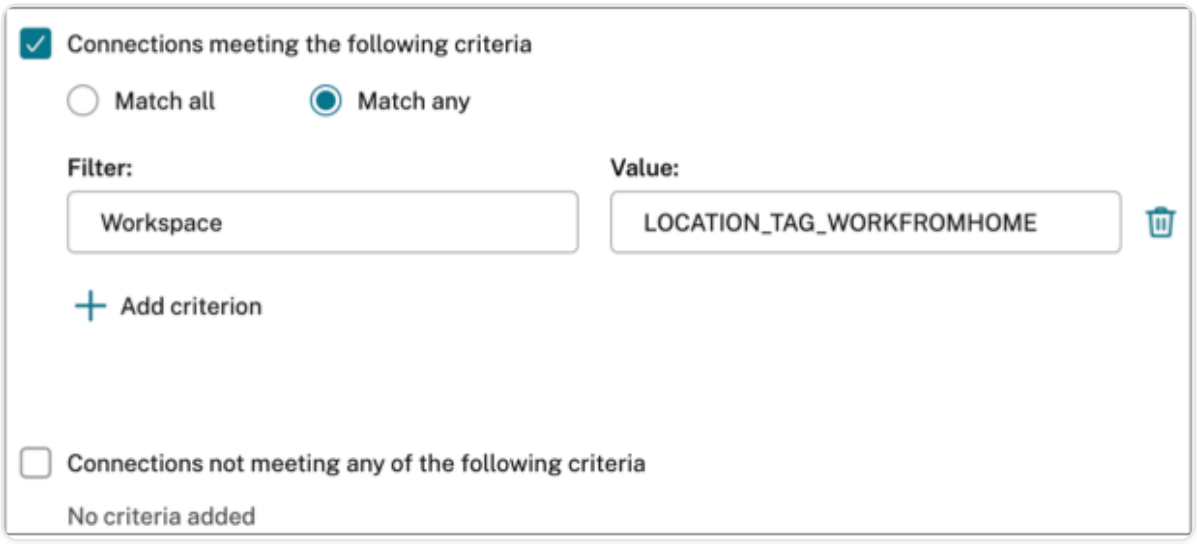
> entanto, ao definir tags no Citrix Studio, você deve prefixar o nome da tag com “LOCATION_TAG”. Por exemplo, “LOCATION_TAG_BRANCHOFFICE”.

Use as tags definidas em grupos de entrega para enumeração de aplicativos

1. Faça login no Citrix Cloud.
2. No bloco **Citrix DaaS**, clique em **Gerenciar**.
3. Crie um grupo de entrega. Para obter detalhes, consulte Criar grupos de entrega.
4. Selecione o grupo de entrega que você criou e clique em **Editar Grupo de Entrega**.
5. Clique em **Política de Acesso**.
6. Para clientes que usam acesso adaptativo, execute as seguintes etapas para restringir o acesso de um grupo de entrega apenas a redes internas:
   a. Clique com o botão direito do mouse no grupo de entrega e selecione **Editar**.
   b. Selecione a política de acesso no painel esquerdo.
   c. Clique no ícone de edição para modificar a política padrão de conexões do Citrix Gateway.



   d. Na página **Editar política**, selecione **Conexões que atendem aos seguintes critérios**, selecione **Corresponder a qualquer**, e então adicione os critérios.



Para usuários WorkFromHome, insira os seguintes valores no respectivo controlador de entrega.

Filtro: Espaço de Trabalho

Valor: LOCATION_TAG_WORKFROMHOME

Para usuários de filial, insira os seguintes valores no respectivo controlador de entrega.

Filtro: Espaço de Trabalho

Valor: LOCATION_TAG_BRANCHOFFICE

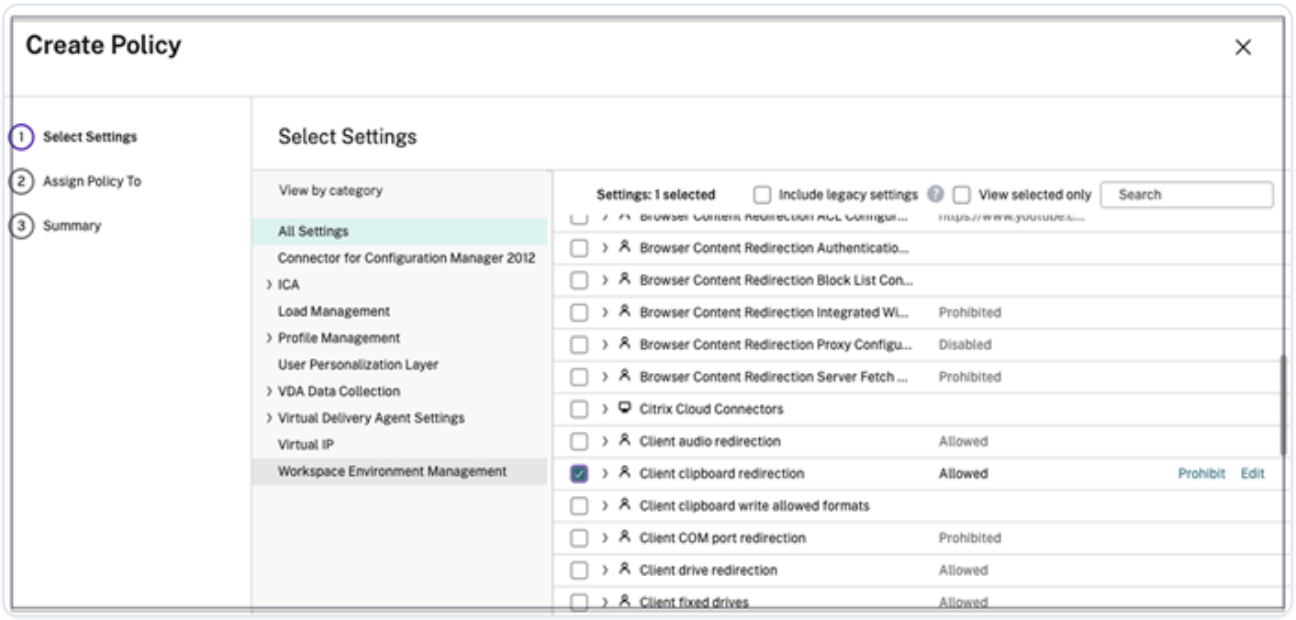
Nota:

- Certifique-se de que, no campo **Valor**, você insira o nome correto da tag de localização, conforme definido ao criar políticas de localização de rede, prefixado por "LOCATION_TAG". Por exemplo, se você definiu a tag de localização como "BRANCHOFFICE", então você deve inserir "LOCATION_TAG_BRANCHOFFICE" no campo **Valor**. As tags de localização de rede nos grupos de entrega devem ser inseridas em maiúsculas, independentemente de como foram definidas na política de localização de rede. Para obter detalhes sobre a configuração de tags de localização, consulte Configurar políticas de localização de rede.
- As tags de localização de rede nos grupos de entrega devem ser inseridas em maiúsculas, independentemente de como foram definidas na política de localização de rede. Para obter detalhes sobre a configuração de tags de localização, consulte Configurar as políticas de localização de rede.

(Opcional) Impor controles inteligentes em aplicativos

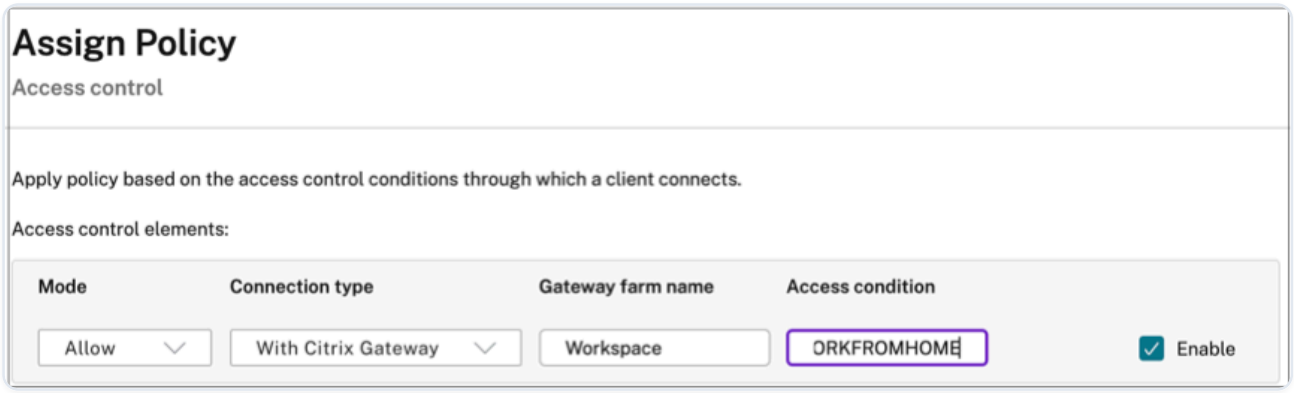
Além de restringir o acesso usando tags de localização de rede, os administradores também podem impor controles inteligentes em aplicativos. Neste exemplo, o redirecionamento da área de transferência do cliente é desabilitado para usuários da localização WorkFromHome.

1. Faça login no Citrix DaaS.
2. navegar até **Políticas** e clique em **Criar Política**.
3. Selecione **Redirecionamento da área de transferência do cliente** e, em seguida, clique em **Proibir**.
4. Clique em **Avançar**.



1. Na página **Atribuir política a**, selecione **Controle de acesso**.
2. Defina os seguintes valores para a política:

   - Modo: **Permitir**
   - Tipo de conexão: **Com Citrix Gateway**
   - Nome do farm do Gateway: **Workspace**
   - Condição de Acesso: **LOCATION_TAG_WORKFROMHOME** (tudo em maiúsculas)



1. Clique em **Avançar**.
2. Insira um nome para a política e adicione uma descrição da política.
3. Clique em **Concluir**.

Usuários do local **WORKFROMHOME** não podem realizar acesso à área de transferência para seus recursos iniciados.

Tags de localização de rede

O serviço de Localizações de Rede fornece as seguintes tags.

- **Tags padrão:** Essas tags são definidas no serviço de Localizações de Rede. As seguintes tags padrão estão disponíveis.
  - **LOCATION_internal:** Tag enviada por padrão quando o tipo de conectividade de rede é definido como **Interna** ao definir uma localização de rede.
  - **LOCATION_external:** Tag enviada por padrão quando o tipo de conectividade de rede é definido como **Externo** ao definir um local de rede.
  - **LOCATION_undefined:** Tag enviada para um endereço IP que não está definido na política, mas que está vindo através do serviço de Locais de Rede. O lançamento para esses usuários é o mesmo que o definido no grupo de recursos.
- **Tags personalizadas:** Os administradores podem definir nomes de tags personalizadas nas políticas. Exemplo: home, Office, BRANCH

> **Observação:**
>
> - Ao definir tags para o serviço de Localização de Rede, certifique-se do seguinte:

As tags padrão sempre começam com o prefixo "LOCATION_ `<tag name>`. Por exemplo, LOCATION_INTERNAL.

As tags personalizadas sempre começam com o prefixo "LOCATION_TAG `<tag name>`. Por exemplo, LOCATION_TAG_OFFICE.

- Ao definir tags nos grupos de entrega, as tags devem ser inseridas em maiúsculas.

  Tags padrão: LOCATION_INTERNAL, LOCATION_EXTERNAL, LOCATION_UNDEFINED

  Tags personalizadas: LOCATION_TAG_OFFICE, LOCATION_TAG_HOME

A tabela a seguir resume as políticas e tags para o cenário mencionado anteriormente.

LOCALIZAÇÃO	POLÍTICA	TAG PERSONALIZADA	TAG PADRÃO	TAG A SER USADA NO GRUPO DE ENTREGA DAAS	TAGS A SEREM USADAS NA POLÍTICA DE ACESSO INTELIGENTE
WFH	WFH	WORKFROMHOME	LOCATION_EXTERNAL	LOCATION_WORKFROMHOME e/ou LOCATION_EXTERNAL	LOCATION_WORKFROMHOME e/ou LOCATION_EXTERNAL
BranchOffice	BranchOffice	BRANCHOFFICE	LOCATION_EXTERNAL	LOCATION_BRANCHOFFICE e/ou LOCATION_EXTERNAL	LOCATION_BRANCHOFFICE e/ou LOCATION_EXTERNAL
Outro	Não definido	Não definido	LOCATION_UNDEFINED	LOCATION_UNDEFINED	LOCATION_UNDEFINED

Problemas conhecidos

Se você desativar o recurso Acesso Adaptativo depois que ele foi ativado e as regras foram definidas (tags e tipo de conectividade), isso não remove os locais da página Locais de Rede, embora as tags de local e as colunas de tipo de conectividade estejam ocultas. Mas esses locais são desativados no back-end. Este é um problema cosmético.

Configurar políticas de gravação de sessão com base em tags

Gravação de Sessão permite que as organizações gravem a atividade do usuário na tela em sessões virtuais. Você pode especificar tags, incluindo tags de localização de rede, ao criar uma política de gravação de sessão personalizada, política de detecção de eventos ou política de resposta a eventos. Para um exemplo, consulte Criar uma política de gravação personalizada.

Aplicativos

Introdução

Se sua implantação usa apenas grupos de entrega (e não grupos de aplicativos), adicione aplicativos diretamente aos grupos de entrega. Quando os grupos de aplicativos estão disponíveis, é melhor adicionar aplicativos a eles, pois essa prática simplifica a administração. Todo aplicativo deve ser associado a pelo menos um grupo de entrega ou grupo de aplicativos.

No assistente **Adicionar Aplicativos**, você pode selecionar um ou mais grupos de entrega, ou um ou mais grupos de aplicativos, mas não ambos. Embora você possa alterar posteriormente a associação de grupo de um aplicativo (por exemplo, mover um aplicativo de um grupo de aplicativos para um grupo de entrega), a melhor prática desencoraja adicionar essa complexidade. Mantenha seus aplicativos em um único tipo de grupo.

Quando você associa um aplicativo a mais de um grupo, um problema de visibilidade pode ocorrer se você não tiver permissão suficiente para visualizar o aplicativo em todos esses grupos. Nesses casos, consulte um administrador com maiores permissões ou solicite que seu escopo seja estendido para incluir todos os grupos aos quais o aplicativo está associado.

Se você publicar dois aplicativos com o mesmo nome (talvez de grupos diferentes) para os mesmos usuários, altere a propriedade `Application name (for user)` no Studio. Caso contrário, os usuários verão nomes duplicados no aplicativo Citrix Workspace™.

Você pode alterar as propriedades (configurações) de um aplicativo ao adicioná-lo ou posteriormente. Você também pode alterar a pasta do aplicativo onde o aplicativo é colocado, seja ao adicionar o aplicativo ou posteriormente.

Adicionar aplicativos

Você pode adicionar aplicativos ao criar ou editar um grupo de entrega ou grupo de aplicativos. O procedimento a seguir descreve como adicionar aplicativos depois de criar um grupo.

É bom saber:

- Você não pode adicionar aplicativos a grupos de entrega de Acesso Remoto para PC.
- Você não pode usar o assistente **Adicionar Aplicativo** para remover aplicativos de grupos de entrega ou grupos de aplicativos. Essa é uma operação separada.

Adicionar um ou mais aplicativos a vários grupos de entrega ou grupos de aplicativos

Para adicionar aplicativos a vários grupos, siga estas etapas:

1. No painel esquerdo, escolha onde você deseja adicionar os aplicativos:
    - Para adicionar a um grupo de entrega, clique em **Grupos de entrega** e selecione o grupo de entrega de destino.
    - Para adicionar a um grupo de aplicativos, clique em **Aplicativos**, selecione a guia **Grupo de aplicativos** e selecione o grupo de aplicativos.
2. Selecione **Adicionar Aplicativos** na barra de ações. O assistente Adicionar Aplicativos é iniciado com uma página de **Introdução**. Clique em **Avançar**.
3. Siga as etapas do assistente para configurar as definições:
    a. Na página **Grupo**, escolha os grupos de entrega e o grupo de aplicativos onde você deseja adicionar aplicativos e clique em **Avançar**. Para obter mais informações, consulte Selecionar grupos.
    b. Na página **Aplicativos**, especifique os aplicativos que você deseja adicionar e clique em **Avançar**. Para obter mais informações, consulte Especificar aplicativos.
    c. Na página **Resumo**, revise as configurações:
        - Se você estiver adicionando 10 ou menos aplicativos, seus nomes serão listados em **Aplicativos a adicionar**
        - Se você estiver adicionando mais de 10 aplicativos, o número total será especificado.
    d. Clique em **Concluir**.

Adicionar um ou mais aplicativos a um grupo de entrega ou grupo de aplicativos

Para adicionar aplicativos a um grupo, siga estas etapas:

1. No painel esquerdo, escolha onde você deseja adicionar os aplicativos:
    - Para adicionar a um grupo de entrega, clique em **Grupos de entrega** e selecione o grupo de entrega de destino.
    - Para adicionar a um grupo de aplicativos, clique em **Aplicativos**, selecione a guia **Grupo de aplicativos** e selecione o grupo de aplicativos.
2. Selecione **Adicionar Aplicativos** na barra de ações.
3. Siga as etapas do assistente para configurar as definições:
    a. Na página **Aplicativos**, especifique os aplicativos que você deseja adicionar e, em seguida, clique em **Avançar**. Para obter mais informações, consulte Especificar aplicativos.
    b. Na página **Resumo**, revise as configurações:
        - Se você estiver adicionando 10 ou menos aplicativos, os nomes deles serão listados em **Aplicativos a adicionar**
        - Se você estiver adicionando mais de 10 aplicativos, o número total será especificado.
    c. Clique em **Concluir**.

Selecionar grupos

A página **Grupos** no assistente **Adicionar Aplicativos** lista todos os grupos de entrega no site. Se existirem grupos de aplicativos, tanto os grupos de aplicativos quanto os grupos de entrega serão listados.

Você pode selecionar grupos de entrega ou grupos de aplicativos — mas *não ambos* ao mesmo tempo. Ou seja, você não pode adicionar aplicativos a um grupo de entrega e a um grupo de aplicativos na mesma operação. Se você estiver usando grupos de aplicativos, recomendamos adicionar aplicativos a esses grupos de aplicativos em vez de a grupos de entrega.

Marque a caixa de seleção ao lado de pelo menos um grupo. Cada aplicativo deve ser associado a pelo menos um grupo.

Especificar aplicativos

A página **Aplicativos** no assistente **Adicionar aplicativos** permite especificar quais aplicativos adicionar ao grupo ou grupos selecionados.

Clique em **Adicionar** para exibir as fontes de aplicativos.

- **Do menu Iniciar:** Aplicativos que são descobertos em uma máquina nos grupos de entrega selecionados. Ao selecionar esta fonte, uma nova página é iniciada com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e, em seguida, clique em **OK**.

  Esta origem não pode ser selecionada se você:

  - Selecionar grupos de aplicativos sem grupos de entrega associados.
  - Selecionar grupos de aplicativos com grupos de entrega associados que não contêm máquinas.
  - Selecionar um grupo de entrega que não contém máquinas.

- **Manualmente:** Aplicativos em um VDA no grupo de entrega ou em outro lugar na sua rede. A seleção desta origem abre uma nova página onde você especifica um aplicativo para adicionar das seguintes maneiras:

  - Digite o caminho para o executável, diretório de trabalho, argumentos de linha de comando opcionais e nomes de exibição para administradores e usuários.
  - Selecione um aplicativo de um VDA no grupo de entrega. Para fazer isso, clique em **Procurar**, insira as credenciais para acessar o VDA, aguarde a conexão com o VDA e, em seguida, selecione um aplicativo do VDA. As propriedades do aplicativo selecionado preenchem automaticamente os campos na página.

- **Existente:** Aplicativos adicionados anteriormente ao site. Ao selecionar esta origem, uma nova página é aberta com uma lista de aplicativos descobertos. Marque as caixas de seleção dos aplicativos a serem adicionados e clique em **OK**.

  Esta origem não pode ser selecionada se o site não tiver aplicativos.

- **Pacotes de aplicativos:** Aplicativos nos pacotes de aplicativos App-V, MSIX, MSIX app attach ou FlexApp. Ao selecionar esta origem, a página **Adicionar Aplicativos de Pacotes** é iniciada. Selecione uma origem de pacote de aplicativos, selecione os aplicativos que deseja adicionar na exibição resultante e, em seguida, selecione **OK**. Para obter mais informações, consulte Implantar e entregar aplicativos App-V.
- **Grupo de Aplicativos**: Grupos de aplicativos. Ao selecionar esta origem, uma nova página é iniciada com uma lista de grupos de aplicativos. (Embora a exibição também liste os aplicativos em cada grupo, você pode selecionar apenas o grupo, não aplicativos individuais.)

Todos os aplicativos atuais e futuros nos grupos selecionados são adicionados. Marque as caixas de seleção dos grupos de aplicativos a serem adicionados e clique em **OK**.

Esta origem não pode ser selecionada se (1) não houver grupos de aplicativos, ou (2) se os grupos de entrega selecionados não suportarem grupos de aplicativos (por exemplo, grupos de entrega com máquinas atribuídas estaticamente).

Conforme observado na tabela, algumas origens na lista **Adicionar** não podem ser selecionadas se não houver uma origem válida desse tipo. Origens incompatíveis (por exemplo, você não pode adicionar grupos de aplicativos a grupos de aplicativos) não são incluídas na lista. Aplicativos que já foram adicionados aos grupos que você escolheu não podem ser selecionados.

Você pode alterar as propriedades (configurações) de um aplicativo nesta página ou posteriormente.

Por padrão, os aplicativos adicionados são colocados na pasta de aplicativos nomeada `Applications`. Você pode alterar o aplicativo nesta página ou posteriormente.

Se você tentar adicionar um aplicativo e já existir um com o mesmo nome na mesma pasta, será solicitado que você renomeie o aplicativo que está adicionando. Você pode aceitar o novo nome sugerido, ou recusar e então renomear o aplicativo ou selecionar uma pasta diferente.

Por exemplo, se `app` existir na pasta **Aplicativos**, e você tentar adicionar outro aplicativo chamado `app` a essa pasta, o novo nome `app_1` será sugerido.

Alterar a associação de grupo de um aplicativo

Depois de adicionar um aplicativo, você pode alterar os grupos de entrega e os grupos de aplicativos aos quais o aplicativo está associado.

Você pode arrastar um aplicativo para um grupo adicional. Esta é uma alternativa ao uso de comandos na barra de ações.

Se um aplicativo estiver associado a mais de um grupo de entrega, seja usando um grupo de aplicativos ou diretamente, a prioridade do grupo pode ser usada para especificar a ordem em que vários grupos são avaliados.

Os grupos podem ser excluídos da consideração com base em fatores como política de acesso, listas de usuários ou tags de acesso inteligente, e a máquina específica escolhida do grupo pode ser afetada por fatores como preferência de zona, prontidão de inicialização e quaisquer restrições de tag. Por padrão, todos os grupos têm prioridade 0 (a mais alta). Se os grupos de entrega

tiverem prioridade igual, o grupo de entrega menos carregado será selecionado para iniciar o aplicativo. O balanceamento de carga vertical não é considerado neste caso.

Um aplicativo pode ser associado a grupos de entrega contendo máquinas compartilhadas (não privadas) que podem entregar aplicativos. Você também pode selecionar grupos de entrega contendo máquinas compartilhadas que entregam apenas desktops, se:

- O grupo de entrega contém máquinas compartilhadas e foi criado com uma versão do XenDesktop 7.x anterior a 7.9
- Você tem permissão `Edit delivery group`. O tipo de grupo de entrega é automaticamente convertido para `desktops and applications` quando a caixa de diálogo de propriedades é confirmada.

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione o aplicativo.
2. Selecione **Propriedades** na barra de ações.
3. Selecione a página **Grupos**.
    - Para adicionar um grupo, clique em **Adicionar** e selecione **Grupos de Aplicativos** ou **Grupos de Entrega**. (Se você não criou nenhum grupo de aplicativos, a única entrada é **Grupos de Entrega**.) Em seguida, selecione um ou mais grupos disponíveis. Grupos que são incompatíveis com o aplicativo, ou que já estão associados ao aplicativo, não podem ser selecionados.
    - Para remover um grupo, selecione um ou mais grupos e clique em **Remover**. Se a remoção de uma associação de grupo resultar no aplicativo não estando mais associado a nenhum grupo, você será alertado de que o aplicativo será excluído.
    - Para alterar a prioridade de um grupo, selecione o grupo e clique em **Editar Prioridade**. Selecione um valor de prioridade e clique em **OK**.
4. Quando terminar, clique em **Aplicar** para aplicar as alterações e deixar a janela aberta, ou clique em **OK** para aplicar as alterações e fechar a janela.

Alterar propriedades do aplicativo

Você pode alterar as propriedades de apenas um aplicativo por vez.

Para alterar as propriedades de um aplicativo:

1. Selecione **Aplicativos** no painel esquerdo.
2. Selecione um aplicativo e, em seguida, selecione **Propriedades** na barra de ações.

3. No painel esquerdo, selecione a página que contém a propriedade que você deseja alterar.
4. Quando terminar, clique em **Aplicar** para aplicar as alterações feitas e manter a janela aberta, ou clique em **Salvar** para aplicar as alterações e fechar a janela.

NOME DA PÁGINA	DESCRIÇÃO
Identificação	Especifique a descrição e os nomes do aplicativo: • Nomes de aplicativos vistos pelo usuário e pelo administrador. • Descrição e, se necessário, palavras-chave para o StoreFront.
Entrega	Especifique como este aplicativo é entregue aos usuários • Ícone • Categoria ou pasta onde um aplicativo aparece em sua loja. • Se deve criar um atalho na área de trabalho do usuário. • Limites. consulte Configurar limites de aplicativo. • Visibilidade de aplicativos empacotados: Citrix Virtual Desktops, Citrix Virtual Apps ou ambos.

NOME DA PÁGINA	DESCRIÇÃO
Localização	Especifique o seguinte local: • Caminho para o executável; consulte Passar parâmetros para aplicativos publicados. • Argumentos de linha de comando; consulte Passar parâmetros para aplicativos publicados. • Diretório de trabalho
Grupos	Adicione, remova ou altere a prioridade dos grupos de entrega ou de aplicativos onde o aplicativo está disponível.
Limitar Visibilidade	Controle quais usuários podem ver o aplicativo no aplicativo Citrix Workspace. Um aplicativo invisível ainda pode ser iniciado. Para torná-lo indisponível e invisível, adicione-o a um grupo diferente. **Nota:** Atualmente, este recurso está disponível apenas para usuários do AD e do Microsoft Entra. Para usuários do Microsoft Entra, a limitação de visibilidade do aplicativo requer a versão 2411 ou posterior do VDA.

NOME DA PÁGINA	DESCRIÇÃO
Associação de Tipo de Arquivo	Especifique quais extensões o aplicativo abre automaticamente.
Zona	Quando seu site inclui várias zonas, especifique se as zonas afetam o lançamento do aplicativo.

As alterações do aplicativo podem não ter efeito para os usuários atuais do aplicativo até que eles saiam de suas sessões.

Configurar limites de aplicativo

Configure limites de aplicativo para ajudar a gerenciar o uso do aplicativo. Por exemplo, você pode usar limites de aplicativo para gerenciar o número de usuários acessando um aplicativo simultaneamente. Da mesma forma, os limites de aplicativo podem ser usados para gerenciar o número de instâncias simultâneas de aplicativos que consomem muitos recursos. Esse limite pode ajudar a manter o desempenho do servidor e evitar a deterioração do serviço.

Este recurso limita o número de lançamentos de aplicativos que são intermediados pelo Controller (por exemplo, do aplicativo Citrix Workspace e do StoreFront), e não o número de aplicativos em execução que podem ser lançados por outros métodos. Isso significa que os limites de aplicativo auxiliam os administradores no gerenciamento do uso simultâneo, mas não fornecem aplicação em todos os cenários. Por exemplo, os limites de aplicativo não podem ser aplicados quando o Controller está no modo de interrupção.

Por padrão, não há limite para quantas instâncias de aplicativo podem ser executadas ao mesmo tempo. Existem várias configurações de limite de aplicativo. Você pode configurar qualquer uma ou todas elas.

- O número máximo de instâncias simultâneas do aplicativo por todos os usuários no grupo de entrega.
- Uma instância do aplicativo por usuário no grupo de entrega.
- O número máximo de instâncias simultâneas do aplicativo por máquina (somente PowerShell).

Se um limite for configurado, uma mensagem de erro será gerada quando um usuário tentar iniciar uma instância do aplicativo que excederá o limite configurado. Se mais de um limite for configurado, um erro será relatado quando o primeiro limite for atingido.

Exemplos usando limites de aplicativo:

- **Limite máximo de instâncias simultâneas:** Em um grupo de entrega, você configura o número máximo de instâncias simultâneas do aplicativo `Alpha` para 15. Mais tarde, os usuários nesse grupo de entrega têm 15 instâncias desse aplicativo em execução ao mesmo tempo. Se qualquer usuário nesse grupo de entrega agora tentar iniciar `Alpha`, uma mensagem de erro será gerada. `Alpha` não é iniciado porque excederia o limite configurado de instâncias simultâneas do aplicativo (15).
- **Limite de um aplicativo por usuário:** Em outro grupo de entrega, você habilita a opção de uma instância por usuário para o aplicativo `Beta`. O usuário Tony inicia o aplicativo `Beta` com sucesso. Mais tarde no dia, enquanto esse aplicativo ainda está em execução na sessão de Tony, ele tenta iniciar outra instância de `Beta`. Uma mensagem de erro é gerada e `Beta` não é iniciado porque excederia o limite de uma instância por usuário.
- **Número máximo de instâncias simultâneas e limites de uma instância por usuário:** Em outro grupo de entrega, você configura um número máximo de instâncias simultâneas de 10 e habilita a opção de uma instância por usuário para o aplicativo `Delta`. Mais tarde, quando 10 usuários nesse grupo de entrega tiverem cada um uma instância de `Delta` em execução, qualquer outro usuário nesse grupo de entrega que tentar iniciar `Delta` receberá uma mensagem de erro. `Delta` não é iniciado. Se qualquer um dos 10 usuários atuais de `Delta` tentar iniciar uma segunda instância desse aplicativo, eles receberão uma mensagem de erro e a segunda instância não será iniciada.
- **Número máximo de instâncias simultâneas por máquina e usando restrições de tag:** O aplicativo `Charlie` tem requisitos de licenciamento e desempenho que ditam quantas instâncias podem estar em execução ao mesmo tempo em um servidor específico. Esses requisitos também ditam quantas instâncias podem estar em execução simultaneamente em todos os servidores do site.

  O limite de instâncias de aplicativo por máquina afeta qualquer servidor no site (não apenas máquinas em um grupo de entrega específico). Digamos que seu site tenha três servidores. Para o aplicativo `Charlie`, você configura o limite de instâncias do aplicativo por máquina para 2. Assim, não mais do que seis instâncias do aplicativo `Charlie` podem ser iniciadas em todo o site. (Isso é um limite de duas instâncias de Charlie em cada um dos três servidores.)

Para restringir o uso de um aplicativo a apenas certas máquinas dentro de um grupo de entrega (além de limitar as instâncias em todas as máquinas em todo o site):

- Use a funcionalidade de marcação para essas máquinas.
- Configure o número máximo de instâncias por limite de máquina para esse aplicativo.

Se os aplicativos forem iniciados por métodos diferentes do agenciamento do Controller (por exemplo, enquanto um Controller estiver em modo de interrupção) e os limites configurados forem excedidos, os usuários não poderão iniciar mais instâncias até que fechem instâncias suficientes para não exceder mais os limites. As instâncias que excederam o limite não são encerradas à força. Elas podem continuar até que seus usuários as fechem.

Se você desabilitar o roaming de sessão, desabilite o limite de um aplicativo por usuário. Se você habilitar o limite de um aplicativo por usuário, não configure nenhum dos dois valores que permitem novas sessões em novos dispositivos. Para obter informações sobre roaming, consulte Sessões.

Para configurar o limite máximo de instâncias por grupo de entrega e o limite de uma instância por usuário:

1. Selecione **Aplicativos** no painel esquerdo e, em seguida, selecione um aplicativo.
2. Selecione **Propriedades** na barra de ações.
3. Na página **Entrega**, escolha uma das seguintes opções.
   - **Permitir uso ilimitado**. Não há limite para o número de instâncias em execução ao mesmo tempo. Este é o padrão.
   - **Definir limites para o aplicativo**. Existem dois tipos de limite; especifique um ou ambos.
     - Especifique o número máximo de instâncias que podem ser executadas simultaneamente por máquina
     - Limitar a uma instância do aplicativo por usuário
4. Clique em **OK** para aplicar a alteração e fechar a caixa de diálogo, ou em **Aplicar** para aplicar a alteração e deixar a caixa de diálogo aberta.

Para configurar o limite máximo de instâncias por máquina (somente PowerShell):

- No PowerShell (usando o Remote PowerShell SDK para implantações do Citrix Cloud™ ou o PowerShell SDK para implantações locais), insira o cmdlet `BrokerApplication` apropriado com o parâmetro `MaxPerMachineInstances`.

- Para obter orientação, use o cmdlet `Get-Help`. Por exemplo:

```
Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
```

Duplicar, habilitar ou desabilitar, renomear ou excluir um aplicativo

As seguintes ações estão disponíveis:

- **Duplicar:** Você pode querer duplicar um aplicativo para criar uma versão diferente com parâmetros ou propriedades distintas. Ao duplicar um aplicativo, ele é automaticamente renomeado com um sufixo exclusivo e colocado ao lado do original. Você também pode querer duplicar um aplicativo e depois adicioná-lo a um grupo diferente. (Após a duplicação, a maneira mais fácil de mover um aplicativo é arrastando-o.)
- **Habilitar ou desabilitar:** Habilitar e desabilitar um aplicativo é uma ação diferente de habilitar e desabilitar um grupo de entrega ou grupo de aplicativos.
- **Renomear:** Você pode renomear apenas um aplicativo por vez. Se você tentar renomear um aplicativo e já existir um com o mesmo nome na mesma pasta ou grupo, será solicitado que você especifique um nome diferente.
- **Excluir:** Excluir um aplicativo o remove dos grupos de entrega e grupos de aplicativos aos quais estava associado, mas não da origem que foi usada para adicionar o aplicativo originalmente. Excluir um aplicativo é uma ação diferente de removê-lo de um grupo de entrega ou grupo de aplicativos.

Para duplicar, habilitar, desabilitar, renomear ou excluir um aplicativo:

1. Selecione **Aplicativos** no painel esquerdo.
2. Selecione um ou mais aplicativos e, em seguida, selecione a tarefa apropriada na barra de ações.
3. Confirme a ação, quando solicitado.

Remover aplicativos de um grupo de entrega

Um aplicativo deve estar associado (pertencer) a pelo menos um grupo de entrega ou grupo de aplicativos. Se você tentar remover um aplicativo de um grupo de entrega que removeria a associação desse aplicativo com qualquer grupo de entrega ou grupo de aplicativos, você será notificado de que o aplicativo será excluído se você continuar. Quando isso acontece, se você quiser entregar esse aplicativo, você deve adicioná-lo novamente de uma fonte válida.

1. Selecione **Grupos de Entrega** no painel esquerdo e, em seguida, selecione um grupo de entrega.

2. Na guia **Aplicativos**, selecione o aplicativo que você deseja remover.
3. Selecione **Remover do Grupo de Entrega** na barra de ações.
4. Confirme a remoção.

Remover aplicativos de um grupo de aplicativos

Um aplicativo deve pertencer a pelo menos um grupo de entrega ou grupo de aplicativos. Se você tentar remover um aplicativo de um grupo de aplicativos que resultará na não pertencimento desse aplicativo a nenhum grupo, você será notificado de que o aplicativo será excluído se você continuar. Quando isso acontece, se você quiser entregar esse aplicativo, você deve adicioná-lo novamente de uma fonte válida.

1. Selecione **Aplicativos** no painel esquerdo.
2. Selecione o grupo de aplicativos e, em seguida, selecione um ou mais aplicativos.
3. Selecione **Remover do Grupo de Aplicativos** na barra de ações.
4. Confirme a remoção.

Passar parâmetros para aplicativos publicados

Use a página **Localização** das propriedades de um aplicativo para inserir a linha de comando e passar parâmetros para aplicativos publicados.

Quando você associa um aplicativo publicado a tipos de arquivo, os símbolos `"%*"` (símbolos de porcentagem e asterisco entre aspas duplas) são anexados ao final da linha de comando do aplicativo. Esses símbolos atuam como um espaço reservado para parâmetros passados para dispositivos de usuário.

Se um aplicativo publicado não iniciar conforme o esperado, verifique se sua linha de comando contém os símbolos corretos. Por padrão, os parâmetros fornecidos pelos dispositivos do usuário são validados quando os símbolos `"%*"` são anexados. Para aplicativos publicados que usam parâmetros personalizados fornecidos pelo dispositivo do usuário, os símbolos `"%**"` são anexados à linha de comando para ignorar a validação da linha de comando. Se você não vir esses símbolos em uma linha de comando para o aplicativo, adicione-os manualmente.

Se o caminho para o arquivo executável incluir nomes de diretório com espaços (como `"C:\Program Files"`), coloque a linha de comando para o aplicativo entre aspas duplas para indicar que o espaço pertence à linha de comando. Para fazer isso, adicione aspas duplas ao redor do caminho e outro conjunto de aspas duplas ao redor dos símbolos `%*`. Certifique-se de incluir um espaço entre a aspa de fechamento para o caminho e a aspa de abertura para os símbolos `%*`.

Por exemplo, a linha de comando para o aplicativo publicado Windows Media Player é:

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **Nota:**
>
> O número máximo de caracteres, incluindo argumentos, na linha de comando para iniciar aplicativos publicados é 203.

Solução de problemas de encerramento de sessão com aplicativos publicados

Ao publicar aplicativos, apenas o arquivo executável principal para o aplicativo publicado é especificado. No entanto, alguns aplicativos podem produzir processos adicionais (filhos) que são executados em segundo plano e não são fechados pelo arquivo executável principal correspondente quando o aplicativo publicado principal é fechado. Processos adicionais também podem ser criados, a partir de scripts executados ou de chaves de registro específicas, como `Run` e `RunOnceKey`. Esses aplicativos podem impedir um encerramento de sessão adequado, resultando em sessões persistentes ou travadas e podem fazer com que a sessão não seja fechada e o usuário seja desconectado.

Nesse caso, você precisa redefinir ou encerrar essas sessões usando o Citrix Director.

Para ajudar a identificar e solucionar problemas de sessões que não estão sendo encerradas corretamente, a Citrix disponibilizou três entradas de registro. A identificação e solução de problemas de sessões que não estão sendo desconectadas corretamente devido a esses problemas é um processo de três etapas:

1. Identificar quais sessões com aplicativos publicados estão impedindo um encerramento de sessão adequado
2. Identificar para esses aplicativos publicados se eles produzem quaisquer processos adicionais (filhos)
3. Adicionar esses processos a uma entrada de registro especificada para evitar que eles impeçam o encerramento da sessão

Etapa 2: Identificar para esses aplicativos publicados se eles produzem quaisquer processos adicionais (filhos)

Uma vez que um aplicativo publicado é identificado como impedindo um encerramento de sessão adequado, o próximo passo é determinar se este aplicativo produz processos adicionais durante a execução.

Você pode ler `HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` para determinar se algum processo está bloqueando um logoff normal quando um aplicativo publicado é fechado.

No exemplo a seguir, a chave `LogoffCheckerBlockingProcess` contém as seguintes entradas:

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

Esses processos atrasaram o logoff normal.

> **Nota:**
>
> Substitua o pelo ID de sessão correto para a sessão que você deseja verificar.

Etapa 3: Adicione esses processos a uma entrada de registro especificada para evitar que eles atrasem o logoff

Você pode adicionar esses processos às seguintes chaves de registro para evitar que eles atrasem o logoff em sessões futuras:

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using
the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules
```

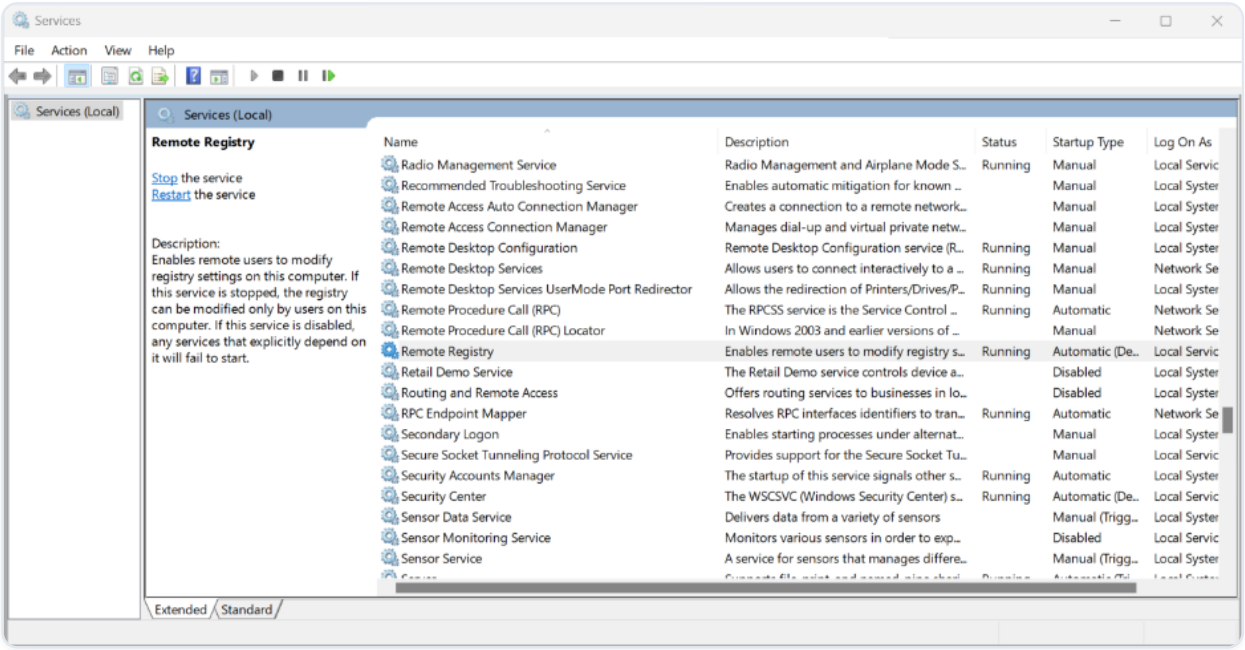
```
Type:REG_SZ

String:MyAppName.exe
```

Para obter mais informações sobre `LogoffCheckSysModules`, consulte Logoff normal de um aplicativo publicado deixa a sessão em estado ativo.

Guia de solução de problemas passo a passo

1. Inicie o Serviço de Registro Remoto no VDA em teste:
    a. No Painel de Controle, selecione **Ferramentas Administrativas > Serviços**.
    b. Clique com o botão direito do mouse em **Serviço de Registro Remoto** e selecione **Propriedades**.
    c. Em **Tipo de inicialização**, selecione **Automático** no menu suspenso.

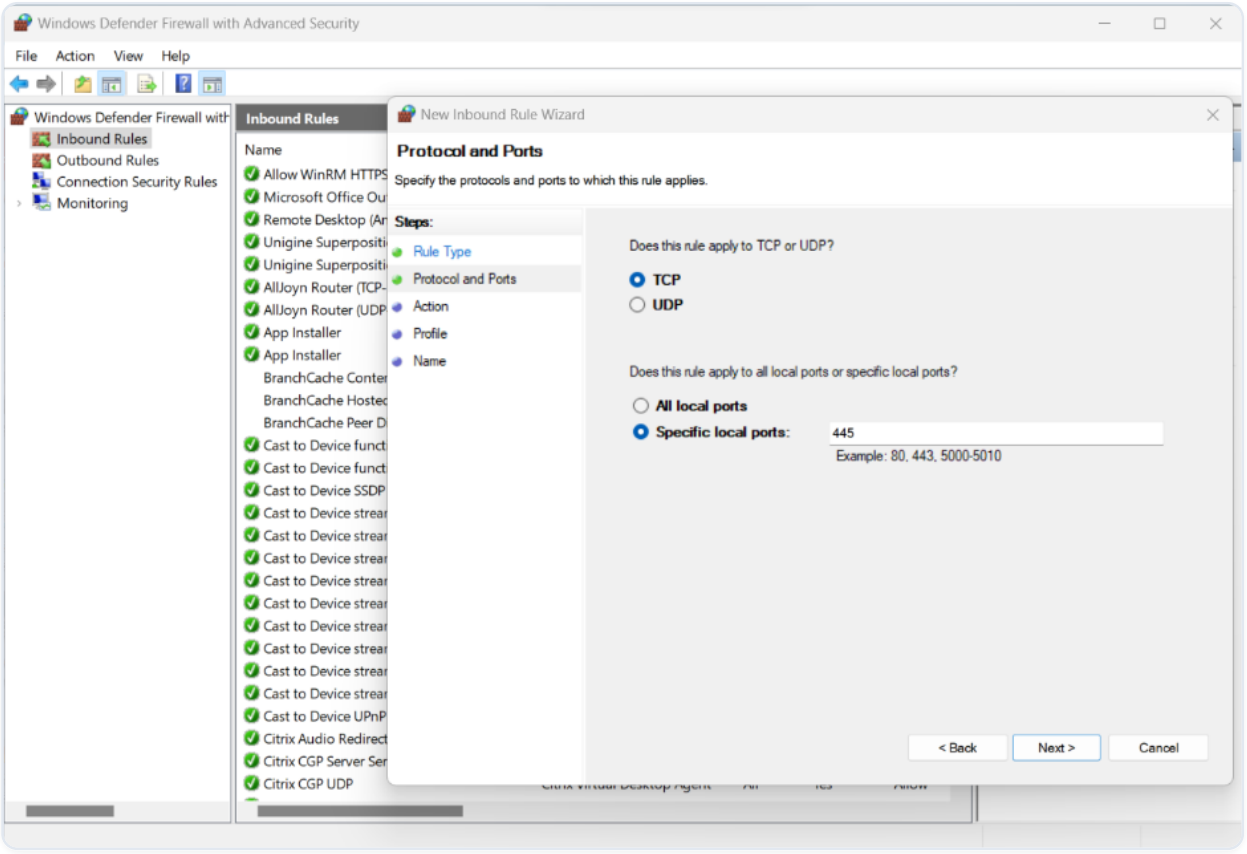


2. Desative o Firewall do Windows no VDA em teste ou crie uma regra de firewall de entrada para habilitar a porta 455:
    a. No Painel de Controle, selecione **Windows Defender Firewall > Configurações Avançadas**.
    b. Clique com o botão direito em **Regras de Entrada** e selecione **Nova Regra**.
    c. No **Assistente de Nova Regra de Entrada**, selecione **Porta**.
    d. Na página **Protocolos e Portas**, selecione **TCP e Portas Locais Específicas**. Insira `445` como a porta local.

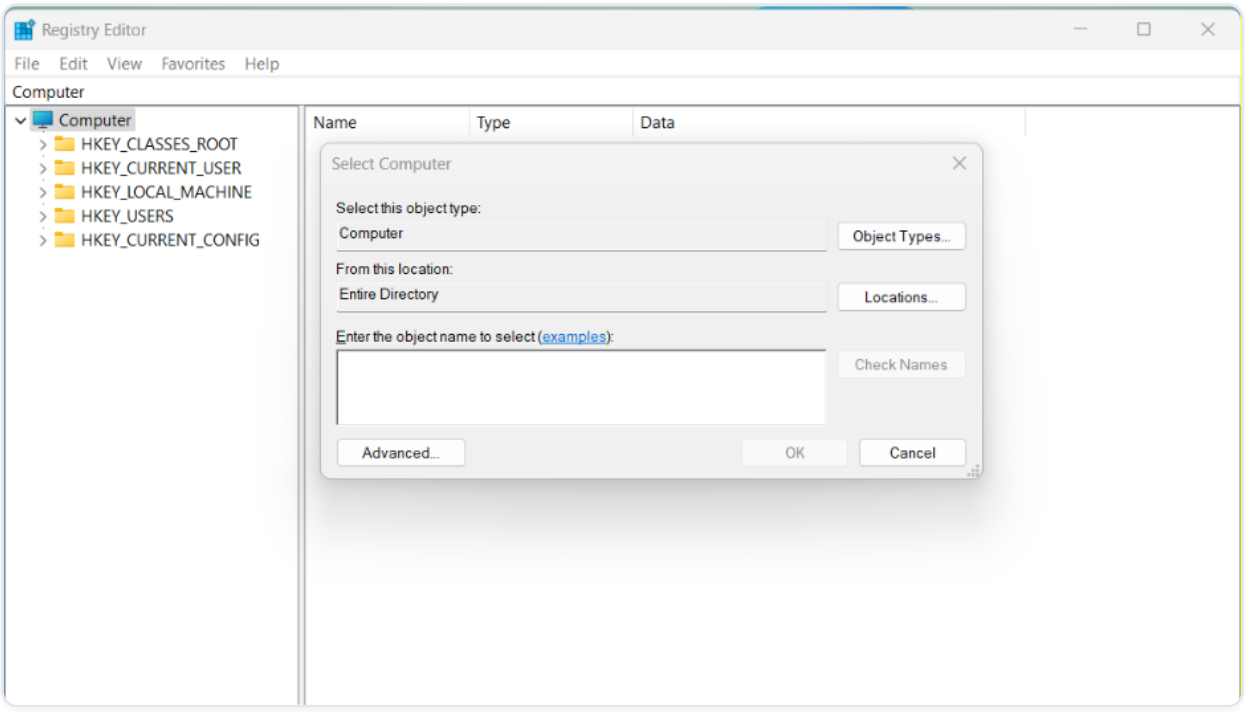
e. Selecione **Permitir Conexão** na página **Ação**.

f. Selecione os perfis de firewall aos quais você deseja aplicar a nova regra de entrada.

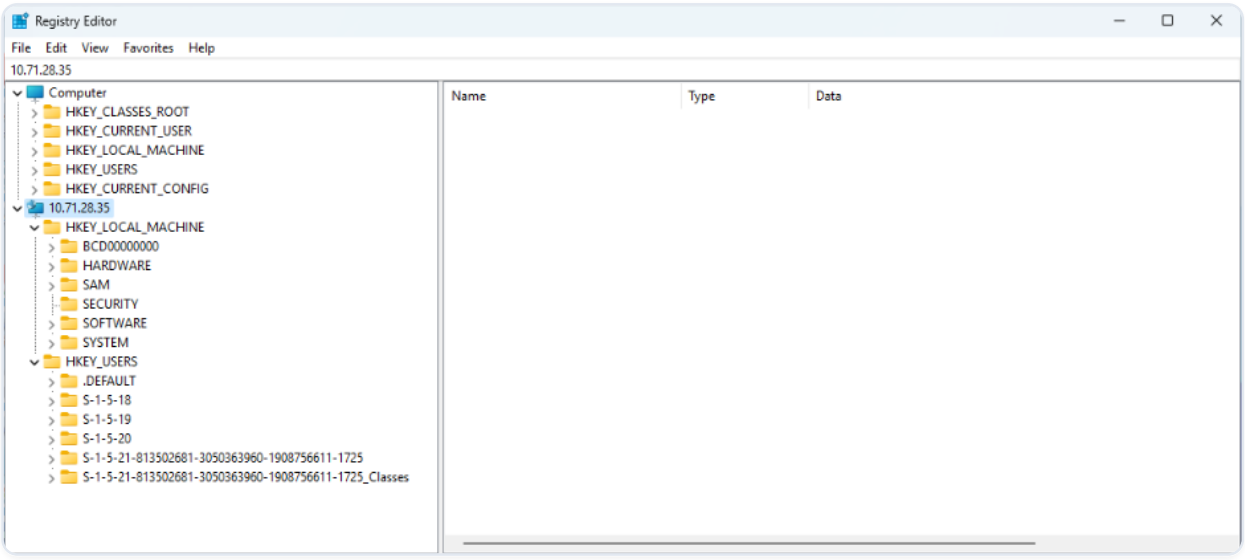
g. Nomeie a regra de firewall e selecione **Concluir** para sair do **Assistente de Nova Regra de Entrada**.



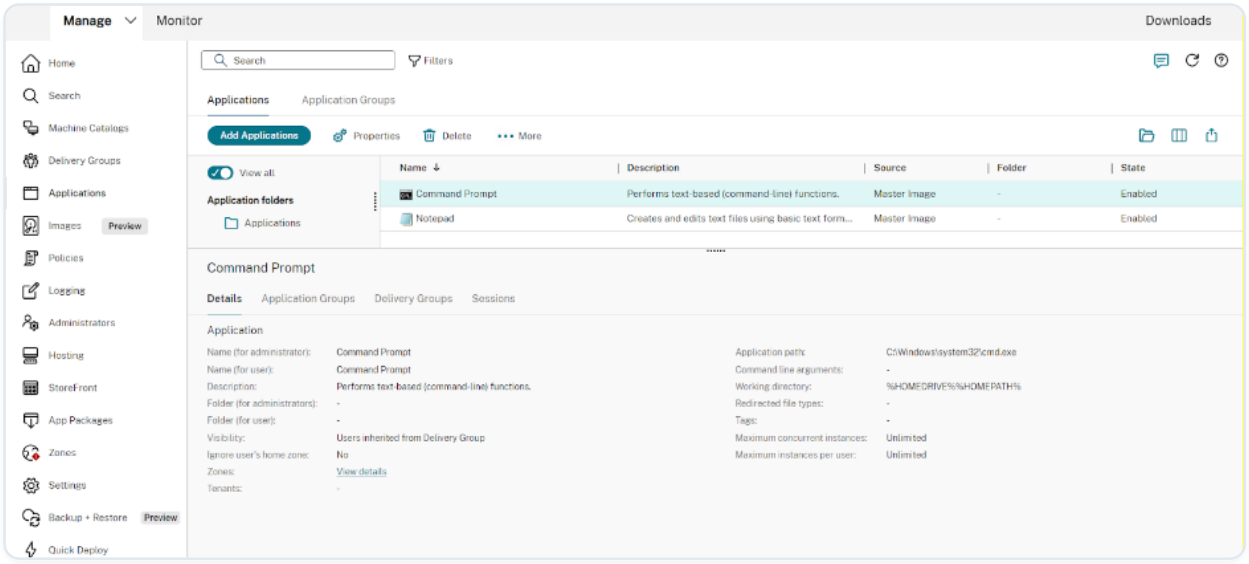
3. De outra VM no mesmo domínio (pode ser DC, DDC ou outro VDA), execute `Regedit` e conecte-se a um registro remoto.



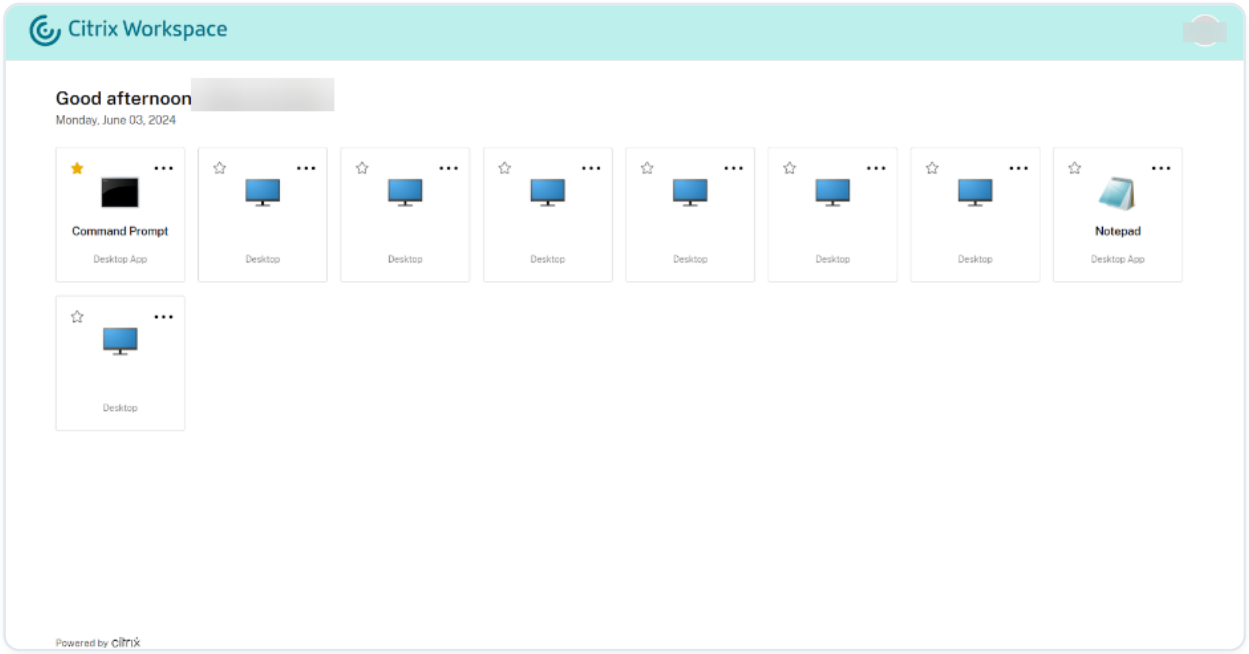
4. Insira o endereço IP do VDA em teste e clique em **OK**. A árvore `regedit` deve exibir ramificações para o VDA em teste.



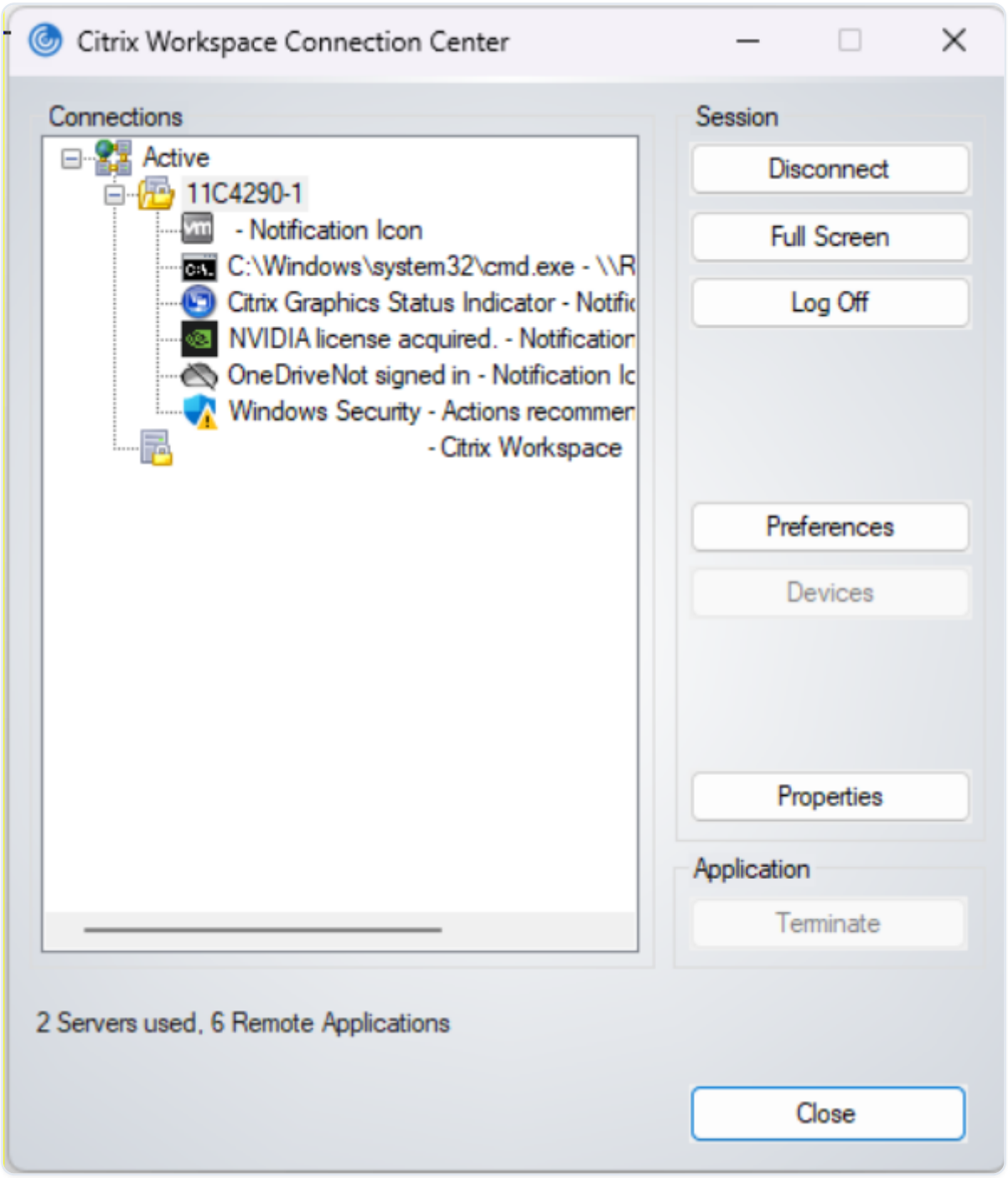
5. Abra o aplicativo publicado **Prompt de Comando**.



O aplicativo **Prompt de Comando** é exibido no aplicativo Citrix Workspace.



6. Abra o **Connection Center** no cliente. Isso é usado para monitorar quando uma sessão é encerrada, após fechar um aplicativo contínuo aberto. Podemos ver na imagem a seguir que o processo do Prompt de Comando `c:\Windows\system32\cmd.exe` está ativo no VDI remoto.

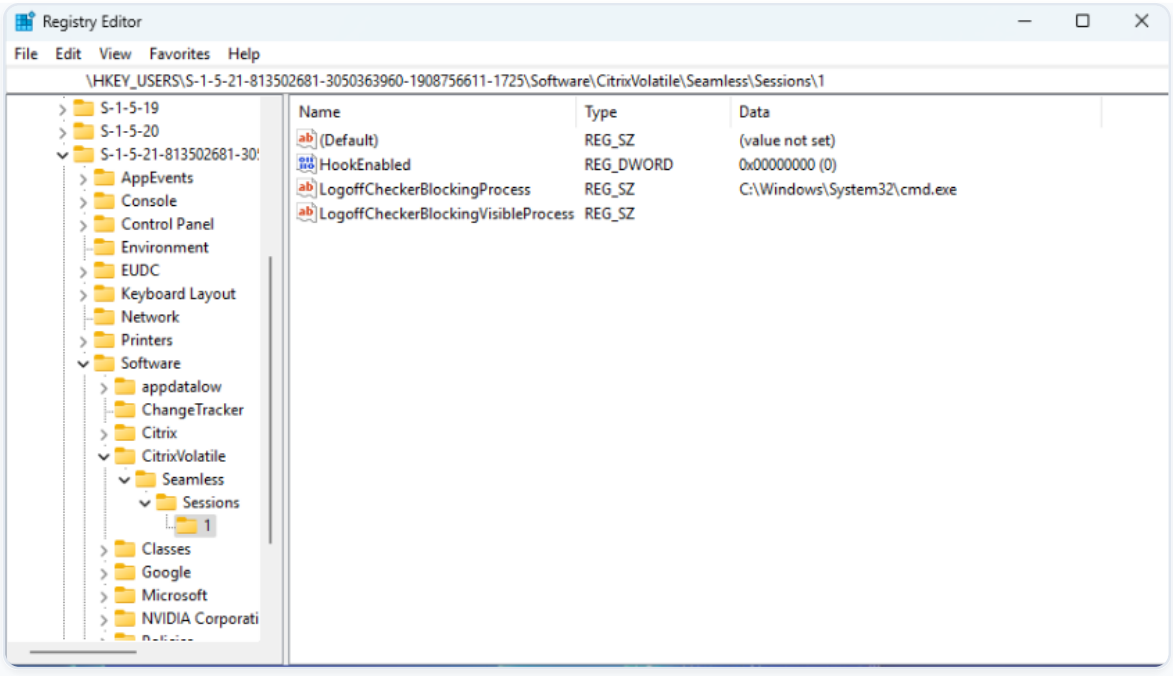


7. No VDA onde o **regedit** está sendo executado, vá para o seguinte local de IP remoto:
   `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

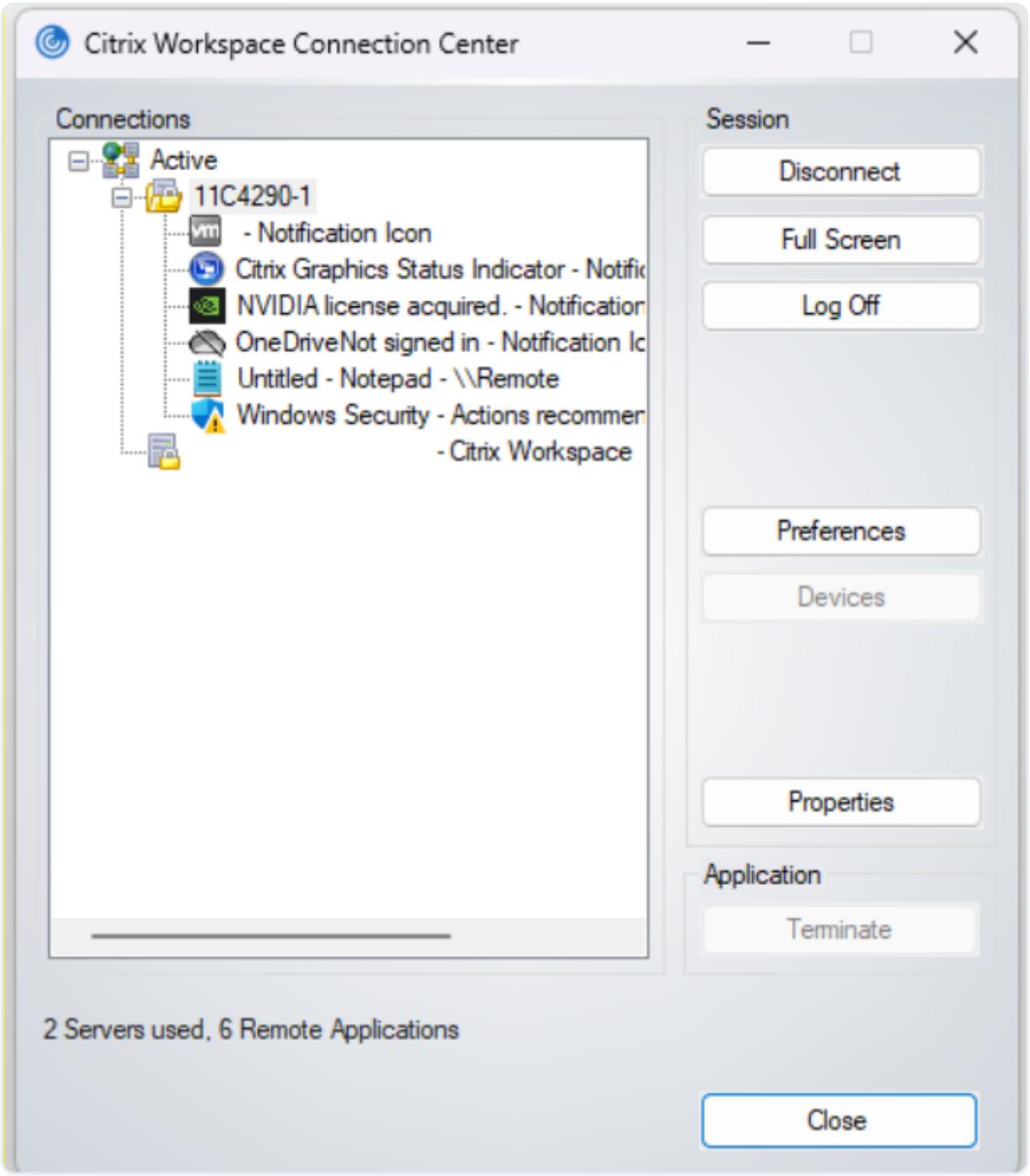
> **Nota:**
>
> Este caminho muda toda vez que você abre uma nova sessão.

8. Existem duas chaves para ler aqui (não as altere aqui): **LogoffCheckBlockingProcess** e **LogoffCheckerBlockingVisibleProcess**. Essas chaves exibem quaisquer programas que estejam bloqueando o encerramento da sessão. A primeira deve exibir `C:\Windows\System32\cmd.exe` já que estava aberta e ainda não foi fechada.

> **Nota:**
>
> **LogoffCheckBlockingProcess** e **LogoffCheckerBlockingVisibleProcess** não devem ser editadas manualmente. A edição manual desses valores de registro pode levar a sessões instáveis.

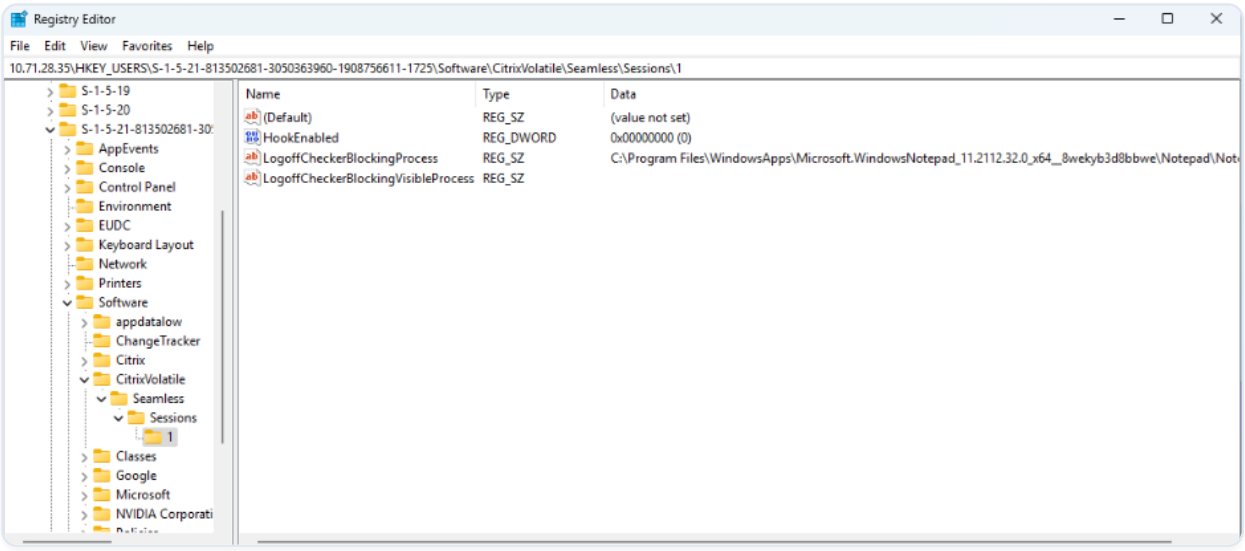


9. Clique em **X** no canto superior direito para sair do **Seamless CMD**.
10. Verifique o centro de conexão para ver se a sessão é encerrada. Pode levar até 30 segundos para fechar. Se for encerrada, significa que não houve aplicativos ou processos que impediram um encerramento de sessão normal.



11. Se a sessão não fechou, atualize a saída do **regedit** com F5.
12. Verifique novamente o conteúdo de **LogoffCheckBlockingProcess** e **LogoffCheckerBlockingVisibleProcess**. O CMD não deve mais estar presente, mas deve haver outro processo listado. Qualquer processo que esteja atualmente bloqueando o encerramento da sessão deve ser exibido aqui.

    Neste caso, **Notepad.exe** está aberto a partir do prompt de comando publicado antes que o prompt de comando fosse fechado e este processo remoto do notepad está impedindo um logoff suave.



13. Anote o caminho para este executável e em qual chave ele apareceu, e insira-o na seguinte chave de registro, sob a árvore remota:

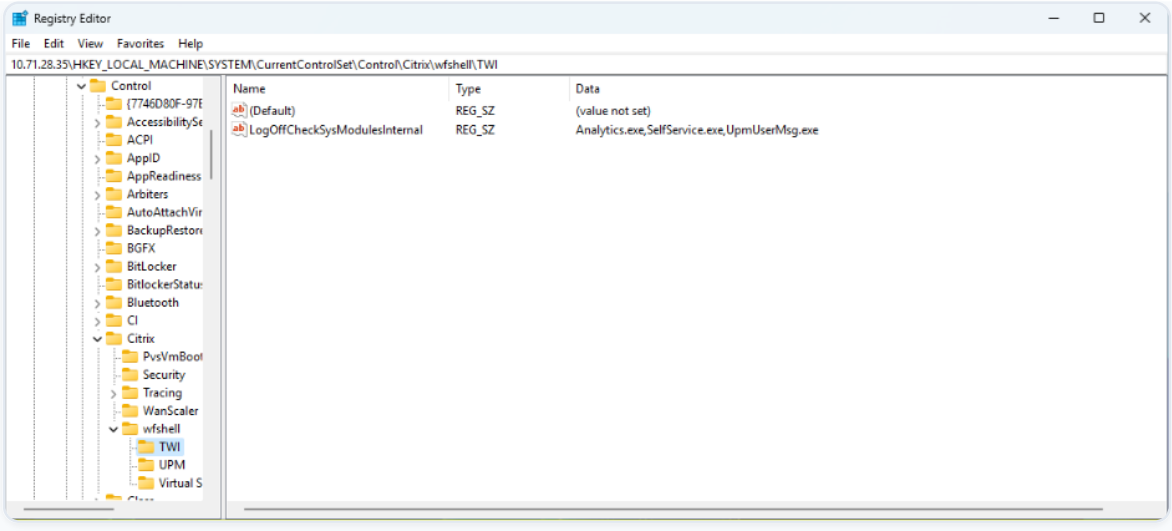
    - Se aparecer em **LogoffCheckBlockingProcess**:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - Se aparecer em **LogoffCheckerBlockingVisibleProcess**:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **Nota:**
>
> Se já houver uma ou mais entradas na chave, adicione uma vírgula no final e coloque a nova entrada após a vírgula.



14. Saia da sessão a partir do centro de conexão no cliente e reabra o Aplicativo Remoto.

15. Repita os passos 9-16 até que a sessão seja encerrada automaticamente em 30 segundos após fechar o Aplicativo Remoto.

> **Nota:**
>
> Após a solução de problemas, reverta as alterações temporárias do Firewall para permitir o acesso remoto ao registro, se necessário.

Como modificar o LogonUI para visualizar a mensagem de isenção de responsabilidade do Windows em tamanho real ao abrir aplicativos publicados

A escala da janela **LogonUI** é aprimorada para cenários onde a autenticação pass-through não ocorre. A janela **LogonUI** é dimensionada com base na resolução do monitor e nas configurações de DPI usadas, o que garante que a janela **LogonUI** completa seja visível sem nenhum corte.

O tamanho da janela em pixels também pode ser definido manualmente no registro.

1. Abra o **Editor do Registro** usando `regedit` no comando **Executar**.
2. Vá para `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`.
3. Crie duas novas chaves DWORD: **LogonUIWidth** e **LogonUIHeight**.
4. Defina o valor das chaves para a largura e altura necessárias em pixels para a janela **LogonUI**.

   Ao definir manualmente o tamanho da janela **LogonUI**, o dimensionamento automático é desativado.

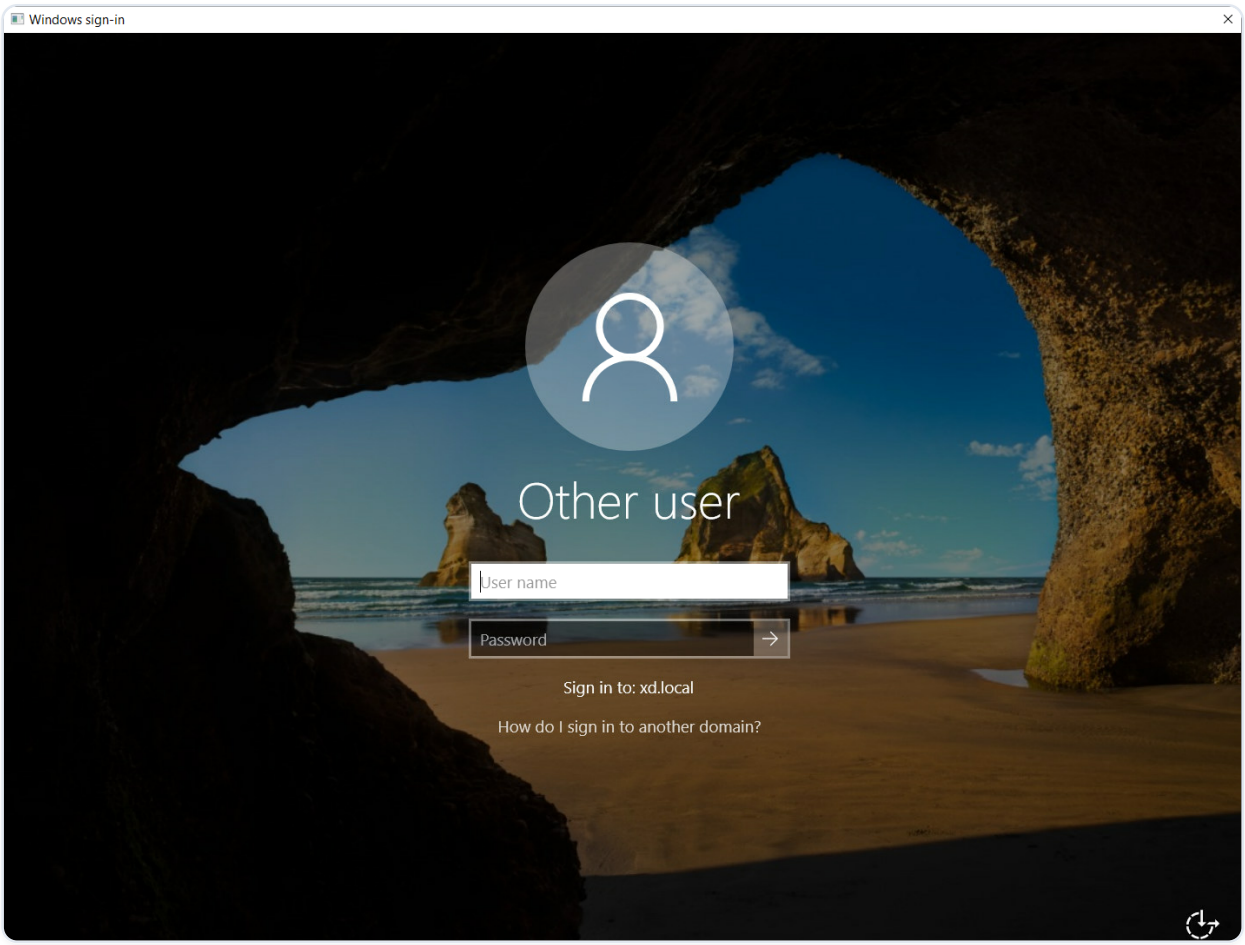
> **Nota:**
>
> Esses caminhos de registro foram alterados a partir da versão 2407 e posteriores. Os valores de registro antigos são ignorados e preteridos.

> Por padrão, a janela **LogonUI** inclui uma barra de título com um botão de fechar que permite ao usuário final desconectar-se da sessão, se necessário.

Desabilitar uma barra de título

Você pode desabilitar a barra de título na janela **LogonUI** com a seguinte chave de registro:

1. Abra o Editor do Registro usando `regedit` no comando **Executar**.
2. Vá para `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`.
3. Crie novas chaves DWORD: **LogonUICaption** e defina o valor da chave como `0`.



Gerenciar pastas de aplicativos

Por padrão, novos aplicativos que você adiciona a grupos de entrega são colocados em uma pasta chamada **Aplicativos**. Você pode especificar uma pasta diferente ao criar o grupo de entrega, ao adicionar um aplicativo ou posteriormente.

É bom saber:

- Você não pode renomear ou excluir a pasta Aplicativos, mas pode mover todos os aplicativos que ela contém para outras pastas que você criar.
- Um nome de pasta pode conter de 1 a 64 caracteres. Espaços são permitidos.

- As pastas podem ser aninhadas em até cinco níveis.
- As pastas não precisam conter aplicativos. Pastas vazias são permitidas.
- As pastas são listadas em ordem alfabética no Web Studio, a menos que você as mova ou especifique um local diferente ao criá-las.
- Você pode ter mais de uma pasta com o mesmo nome, desde que cada uma tenha uma pasta pai diferente. Da mesma forma, você pode ter mais de um aplicativo com o mesmo nome, desde que cada um esteja em uma pasta diferente.
- Você deve ter permissão `View Applications` para ver os aplicativos nas pastas, e deve ter permissão `Edit Application Properties` para todos os aplicativos na pasta para remover, renomear ou excluir uma pasta que contém aplicativos.
- A maioria dos procedimentos a seguir solicita ações usando a barra de ações no Web Studio. Alternativamente, você pode usar menus de clique com o botão direito ou arrastar o item. Por exemplo, se você criar ou mover uma pasta para um local que não pretendia, pode arrastá-la/soltá-la para o local correto.
- Todos os nós no Studio (como **Catálogos de Máquinas**, **Grupos de Entrega**, **Aplicativos** e **Grupos de Aplicativos**) compartilham a mesma árvore de pastas no back-end. Para evitar conflitos de nomes ao renomear ou mover pastas, use nomes exclusivos para pastas de primeiro nível em diferentes nós.

  Se você criar uma pasta usando o cmdlet SDK `New-BrokerAdminFolder` e quiser que ela apareça sob o nó **Aplicativos**, você deve adicionar os metadados `ContainsApplications` usando o cmdlet `Set-BrokerAdminFolderMetadata`.

  Exemplo:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplications -Value true
  ```

Para gerenciar pastas de aplicativos, selecione **Aplicativos** no painel esquerdo. Use a lista a seguir para orientação.

- **Para visualizar todas as pastas (excluindo pastas aninhadas):** Clique em **Mostrar tudo** acima da lista de pastas.
- **Para criar uma pasta no nível mais alto (não aninhada):** Selecione a pasta **Aplicativos**. Para colocar a nova pasta em uma pasta existente diferente de **Aplicativos**, selecione essa pasta. Em seguida, selecione **Criar Pasta** na barra de ações. Insira um nome.

- **Para mover uma pasta:** Selecione a pasta e, em seguida, selecione **Mover Pasta** na barra de ações. Você pode mover apenas uma pasta por vez, a menos que a pasta contenha pastas aninhadas. (A maneira mais fácil de mover uma pasta é arrastá-la.)
- **Para renomear uma pasta:** Selecione a pasta e, em seguida, selecione **Renomear Pasta** na barra de ações. Insira um nome.
- **Para excluir uma pasta:** Selecione a pasta e, em seguida, selecione **Excluir Pasta** na barra de ações. Ao excluir uma pasta que contém aplicativos e outras pastas, esses objetos também são excluídos. A exclusão de um aplicativo remove a atribuição do aplicativo do grupo de entrega. Isso não o remove da máquina.
- **Para mover aplicativos para uma pasta:** Selecione um ou mais aplicativos. Em seguida, selecione **Mover Aplicativo** na barra de ações. Selecione a pasta.

Você também pode colocar os aplicativos que está adicionando em uma pasta na página **Aplicativo** ao criar um grupo de entrega ou um grupo de aplicativos. Por padrão, os aplicativos adicionados vão para a pasta **Aplicativos**. Clique em **Alterar** para selecionar ou criar uma pasta.

Controlar o lançamento local de aplicativos em desktops publicados

Quando os usuários iniciam um aplicativo publicado de dentro de um desktop publicado, você pode controlar se o aplicativo é iniciado nessa sessão de desktop ou como um aplicativo publicado. O aplicativo Citrix Workspace procura o caminho de instalação do aplicativo no registro do Windows no VDA e, se presente, inicia a instância local do aplicativo. Caso contrário, uma instância hospedada do aplicativo é iniciada. Se você iniciar um aplicativo que não está instalado no VDA, o aplicativo hospedado será iniciado. Para obter mais informações, consulte início vPrefer.

No PowerShell (usando o SDK do PowerShell Remoto em implantações do Citrix Cloud ou o SDK do PowerShell em implantações locais), você pode alterar essa ação.

No cmdlet `New-Broker` Application ou `Set-BrokerApplication`, use a opção `LocalLaunchDisabled`. Por exemplo:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

Por padrão, o valor dessa opção é falso (`-LocalLaunchDisabled $false`). Ao iniciar um aplicativo publicado de dentro de um desktop publicado, o aplicativo é iniciado nessa sessão de desktop.

Se você definir o valor da opção como verdadeiro (`-LocalLaunchDisabled $true`), o aplicativo publicado será iniciado. Isso cria uma sessão separada e adicional do desktop publicado (usando o aplicativo Citrix Workspace para Windows) para o aplicativo publicado.

Requisitos e limites:

- O valor `ApplicationType` do aplicativo deve ser `HostedOnDesktop`.
- Esta opção está disponível apenas através do SDK PowerShell apropriado. Não está atualmente disponível na interface gráfica do Web Studio.
- Esta opção requer no mínimo: StoreFront 3.14, Citrix Receiver para Windows 4.11 e Delivery Controller 7.17.

Pacotes de aplicativos

Pacotes de aplicativos são implantações de aplicativos pré-configuradas que a Citrix® gerencia. Eles permitem que os aplicativos sejam virtualizados, o que implica que os aplicativos são executados independentemente do sistema operacional e da interface do dispositivo do usuário.

Pacotes de aplicativos simplificam o gerenciamento de aplicativos, reduzem a sobrecarga de TI e garantem que os aplicativos sejam seguros e funcionais durante todo o seu ciclo de vida.

A Citrix oferece suporte às seguintes tecnologias de empacotamento para entregar aplicativos aos usuários:

- Aplicativos App-V
- Aplicativos MSIX e MSIX app attach
- Aplicativos FlexApp
- Aplicativos Elastic App
- Aplicativos Cloudpaging

Este artigo orienta você sobre como implantar e entregar esses aplicativos empacotados em seu ambiente Citrix DaaS™.

Aplicativos App-V

Application Virtualization (App-V) é uma tecnologia da Microsoft que permite que os aplicativos sejam transmitidos e acessados sem a necessidade de instalação no dispositivo do usuário final. O Citrix DaaS pode usar o App-V para entregar aplicativos, fornecendo uma maneira centralizada e eficiente de gerenciar aplicativos em várias máquinas cliente.

Para obter mais informações sobre os componentes e conceitos com os quais você interage ao entregar aplicativos empacotados App-V, consulte a documentação da Microsoft: Visão geral do Application Virtualization (App-V) para cliente Windows.

Termos importantes

- **Servidor de gerenciamento**: Fornece um console centralizado para gerenciar a infraestrutura do App-V e entrega aplicativos virtuais tanto para o Cliente de Área de Trabalho App-V quanto para um Cliente de Serviços de Área de Trabalho Remota. O servidor de gerenciamento do App-V autentica, solicita e fornece a segurança, medição, monitoramento e coleta de dados exigidos pelo administrador. O servidor usa o Active Directory e ferramentas de suporte para gerenciar usuários e aplicativos.
- **Servidor de publicação**: Fornece aos clientes App-V aplicativos para usuários específicos e hospeda o pacote de aplicativos virtuais para streaming. Ele busca os pacotes no servidor de gerenciamento.
- **Arquivos de configuração dinâmica**: Os pacotes App-V podem ser personalizados usando arquivos de configuração dinâmica que, quando aplicados ao pacote, podem ser usados para alterar suas características. Por exemplo, você pode usá-los para definir atalhos e comportamentos extras de aplicativos. Para obter mais informações, consulte Arquivos de configuração dinâmica

Arquivos de configuração dinâmica

O Citrix App-V oferece suporte a ambos os tipos de arquivos de configuração dinâmica. As configurações de arquivo são aplicadas quando o aplicativo é iniciado:

- **Arquivos de Configuração de Implantação** fornecem configuração em toda a máquina para todos os usuários. Espera-se que esses arquivos sejam nomeados `<packageFileName>_DeploymentConfig.xml` e estejam na mesma pasta que o pacote App-V ao qual se aplicam. Esses arquivos são suportados por gerenciamento de administrador único e duplo.
- **Arquivos de Configuração do Usuário** fornecem configuração específica do usuário que suporta personalizações por usuário para o pacote. O Administrador Único suporta arquivos de configuração do usuário nomeados no seguinte formato: `<packageFileName>_[UserSID | Username | GroupSID |GroupName_]UserConfig.xml` e localizados na mesma pasta que o pacote App-V ao qual se aplicam.

  Quando vários arquivos de Configuração do Usuário existem para um pacote específico, eles são aplicados com a seguinte prioridade:

a. SID do Usuário
b. Nome de usuário
c. SID do Grupo AD (O primeiro encontrado vence)
d. Nome do Grupo AD (O primeiro encontrado vence)
e. Padrão

Por exemplo:

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

MyAppVPackage_joeblogs_UserConfig.xml

MyAppVPackage_S-1-5-32-547_UserConfig.xml

MyAppVPackage_Power Users_UserConfig.xml

MyAppVPackage_UserConfig.xml
```

Nota:

A parte específica do usuário do nome do arquivo também pode ocorrer opcionalmente no final (por exemplo, `MyAppVPackage_UserConfig_joeblogs.xml`).

Importante:

Não é possível aplicar alterações à Configuração de Implantação Dinâmica quando há sessões de usuário com um aplicativo no pacote aberto. Você pode aplicar alterações aos arquivos de Configuração Dinâmica do Usuário se outros usuários (mas não o usuário atual) tiverem o aplicativo do pacote aberto.

Local do arquivo de configuração dinâmica

No gerenciamento de administrador único, os componentes do Citrix App-V processam apenas arquivos de configuração dinâmica, que são encontrados na mesma pasta que seu pacote App-V.

Quando os aplicativos do pacote são iniciados, quaisquer alterações nos arquivos de configuração dinâmica correspondentes são reaplicadas. Se seus arquivos de configuração dinâmica estiverem em um local diferente de seus pacotes, use um arquivo de mapeamento para mapear pacotes para seus arquivos de configuração de implantação.

Para criar um arquivo de mapeamento:

1. Abra um novo arquivo de texto.
2. Para cada arquivo de configuração dinâmica, adicione uma linha que especifique o caminho para o pacote usando o formato `<PackageGuid> : path`.

   Por exemplo:

   ```
   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
   ```

3. Salve o arquivo como `ctxAppVDynamicConfigurations.cfg` na mesma pasta que o pacote.

A hierarquia de diretórios inteira no mesmo compartilhamento UNC que o pacote App-V é pesquisada recursivamente para cima para este arquivo toda vez que um aplicativo no pacote é iniciado.

Métodos

Você pode usar os seguintes métodos para entregar e gerenciar pacotes App-V:

- **Administrador Duplo**: Neste método, os servidores Citrix DaaS e App-V trabalham juntos para entregar e gerenciar pacotes. Este método exige que o Citrix DaaS atualize periodicamente a visualização do instantâneo do estado do servidor App-V. Ele incorre em sobrecarga de hardware, infraestrutura e administração. Os servidores Citrix DaaS e App-V devem permanecer sincronizados, particularmente para permissões de usuário.

  Este método funciona melhor em implantações App-V e Citrix estreitamente acopladas. Neste método:

  - **Servidor de gerenciamento App-V** manipula os arquivos de configuração dinâmica
  - **Componente de Entrega de Pacotes de Aplicativos** instalado em máquinas VDA: Gerencia o registro do servidor de publicação apropriado necessário para o lançamento de um aplicativo.

  Isso garante que o servidor de publicação seja sincronizado para o usuário no momento apropriado. O servidor de publicação mantém outros aspectos do ciclo de vida do pacote de

aplicativos (como atualização no logon e grupos de conexão) usando as configurações com as quais ele está configurado.

- **Administrador Único**: Pacotes de aplicativos são armazenados em compartilhamentos de rede. O Citrix DaaS entrega e gerencia pacotes de forma independente.

  Este método reduz a sobrecarga porque os servidores App-V e a infraestrutura de banco de dados não são necessários na implantação.

  Neste método, você armazena pacotes App-V em um compartilhamento de rede e carrega seus metadados desse local para o seu ambiente. O Componente de Entrega de Pacotes de Aplicativos instalado nas máquinas VDA então gerencia e entrega aplicativos da seguinte forma:

  - Processar os Arquivos de Configuração de Implantação e os Arquivos de Configuração do Usuário quando um aplicativo é iniciado.
  - Gerenciar todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Observação:

- Você pode usar um ou ambos os métodos de gerenciamento simultaneamente. Em outras palavras, ao adicionar aplicativos a Grupos de Entrega, os aplicativos podem vir de pacotes App-V localizados em servidores App-V ou em um compartilhamento de rede.
- Se você estiver usando ambos os métodos de gerenciamento simultaneamente, e o pacote App-V tiver um arquivo de configuração dinâmica em ambos os locais, o arquivo no servidor App-V (gerenciamento duplo) será usado.
- Ao selecionar Pacotes de aplicativos no painel de navegação do Web Studio, a exibição mostra nomes e perfis de pacotes. A coluna **Tipo de pacote** indica qual tecnologia é usada para entregar o pacote e onde eles são referenciados na **Biblioteca de Aplicativos**. Ao selecionar um pacote, o painel de detalhes lista os aplicativos e atalhos no pacote.

Aplicativos MSIX e MSIX app attach

MSIX é um formato de pacote de aplicativos do Windows que oferece uma experiência de empacotamento moderna para todos os aplicativos Windows. O MSIX é adequado para vários tipos de aplicativos Windows, incluindo aplicativos Win32, .NET e UWP.

O MSIX app attach utiliza pacotes MSIX que são pré-expandidos em discos rígidos virtuais, que podem ser montados na máquina de destino conforme necessário, em vez de transmitir o conteúdo do pacote. Isso pode melhorar os tempos de implantação, reduzir o tráfego de rede e diminuir as IOPS na máquina de destino, mas requer trabalho adicional para criar e manter os discos de anexação de aplicativos.

O Citrix DaaS entrega aplicativos MSIX e MSIX app attach aos usuários através do **Componente de Entrega de Pacotes de Aplicativos** instalado nas máquinas VDA. Este componente gerencia todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Para obter mais informações sobre MSIX e MSIX app attach, consulte a documentação da Microsoft: documentação MSIX e App Attach no Azure Virtual Desktop respectivamente.

> **Nota:**
>
> - Oferecemos suporte a pacotes MSIX nativos em VDAs de desktop e servidor e a MSIX app attach nos formatos de imagem de disco `.vhd`, `.vhdx` e `.cim` apenas em VDAs de desktop.
> - A Microsoft não oferece uma implementação de AppAttach para o Server 2019. Embora o AppAttach esteja presente no Server 2022 e 2025, a Microsoft não o suporta nessas versões. Portanto, também não oferecemos suporte ao AppAttach no Server 2022 e 2025.
> - Habilite o sideloading no Windows Server 2019.
> - Certifique-se de que os VDAs confiam nos certificados com os quais os pacotes são assinados.

Aplicativos FlexApp

FlexApp é uma solução de camadas de aplicativos desenvolvida pela Liquidware que anexa qualquer aplicativo a uma sessão do Windows sem modificar a imagem base subjacente através do processo tradicional de instalação de aplicativos.

Os aplicativos FlexApp One são encapsulados em um único arquivo compartilhável, permitindo que operem sem a necessidade de uma camada de aplicativo adicional nas sessões do Windows. Os usuários podem iniciar o aplicativo clicando no arquivo contêiner, o que integra rapidamente um ou mais aplicativos em seu espaço de trabalho do Windows.

A Citrix entrega aplicativos FlexApp aos usuários através do Componente de Entrega de Pacotes de Aplicativos e do agente de entrega FlexApp instalados nas máquinas VDA. Esses dois componentes gerenciam todos os aspectos dos ciclos de vida dos pacotes na máquina host.

Aplicativos Elastic App

A tecnologia Elastic App é um recurso do Citrix App Layering que permite atribuir camadas de aplicativos aos usuários dinamicamente no logon, em vez de instalá-las em uma imagem base. Com a tecnologia Elastic App, os aplicativos seguem o usuário em diferentes máquinas virtuais, garantindo que eles sempre tenham acesso aos aplicativos de que precisam sem inchar a imagem mestre.

O Citrix DaaS entrega aplicativos Elastic App aos usuários através do componente Citrix Personalization e do Application Layering Enterprise Layer Manager (ELM). Esses dois componentes gerenciam todos os aspectos dos ciclos de vida dos pacotes na máquina host. Para obter mais informações sobre o Application Layering Enterprise Layer Manager, consulte o documento Citrix App Layering™.

Aplicativos Cloudpaging

Cloudpaging é a tecnologia de streaming de aplicativos da Numecent que entrega aplicativos a uma sessão do Windows sem exigir alterações na imagem base.

Com o Cloudpaging, os aplicativos são iniciados quase instantaneamente porque apenas uma pequena parte do código (geralmente menos de 10%) é transmitida inicialmente. Os componentes restantes são transmitidos em segundo plano quando os usuários os acessam, proporcionando uma experiência contínua.

Para ambientes Citrix, o Componente de Entrega de Pacotes de Aplicativos no VDA funciona com o Numecent Cloudpaging Player para gerenciar o ciclo de vida do aplicativo. O componente Citrix orquestra a entrega, enquanto o Cloudpaging Player lida com o streaming sob demanda e a execução dentro da sessão.

Requisitos de configuração

Considere os seguintes detalhes de configuração:

CLOUDPAGING PLAYER E LOGOFFCHECKSYSMODULES

Ao usar aplicativos virtuais publicados com contêineres Cloudpaging, configure as seguintes definições para permitir que uma sessão faça logoff:

CONFIGURAÇÃO	VALOR
Chave do Registro	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`
Nome do Valor	`LogoffCheckSysModules`
Tipo de Valor	`REG_SZ`
Dados do Valor	`CoreHelper.exe`

URLS PARA LISTA DE PERMISSÕES

Além dos requisitos padrão de inclusão de URL na lista de permissões, os VDAs exigem acesso ao seguinte endpoint:

PARÂMETRO	VALOR
URL	`external-api.cloudpager.net`
Porta	443
Cliente	Módulo PowerShell do Cloudpager
Configuração de Proxy de Encaminhamento para Baseado na Web	• Acesso de saída permitido • Bypass de autenticação necessário
Descrição	Módulo PowerShell do Cloudpager

Opcionalmente, você pode criar um grupo de entrega dedicado com um VDA usado exclusivamente para realizar a descoberta do Cloudpager para limitar as URLs na lista de permissões necessárias. Recomendamos criar um grupo de entrega com uma máquina que tenha a **versão 2511 do VDA ou posterior** e o **Componente de Entrega de Pacotes de Aplicativos** instalados.

Para obter mais informações sobre os requisitos de rede e firewall do Cliente Cloudpager, consulte o artigo da base de conhecimento da Numecent.

Implantar e entregar pacotes de aplicativos

Pré-requisitos

Para oferecer suporte à entrega de aplicativos App-V, MSIX, MSIX app attach, pacotes FlexApp, Elastic App e Cloudpaging, você deve primeiro instalar o **Componente de Entrega de Pacotes de Aplicativos** nas máquinas VDA. Consulte Instalar o Componente de Entrega de Pacotes de Aplicativos em máquinas VDA para obter detalhes.

INSTALAR O COMPONENTE DE ENTREGA DE PACOTES DE APLICATIVOS EM MÁQUINAS VDA

O Componente de Entrega de Pacotes de Aplicativos gerencia o processo de publicação para pacotes de aplicativos nos formatos App-V, MSIX, MSIX app attach, FlexApp, Elastic App e Cloudpaging. Este componente não é instalado por padrão ao instalar um VDA. Você pode instalar o componente durante ou após a instalação do VDA.

Para instalar o componente durante a instalação do VDA, use uma das seguintes maneiras:

- No assistente de instalação, vá para a página **Componentes Adicionais** e selecione a caixa de seleção **Componente de Entrega de Pacotes de Aplicativos**.
- Na interface de linha de comando, use a opção `/includeadditional "Citrix Personalization for App-V – VDA"`.

Para instalar o componente após a instalação do VDA, siga estas etapas:

1. Na máquina VDA, vá para **Painel de Controle > Programas > Programas e Recursos**, clique com o botão direito em **Citrix Virtual Delivery Agent** e selecione **Alterar**.
2. No assistente que aparece, prossiga para a página **Componentes Adicionais** e, em seguida, habilite a caixa de seleção **Componente de Entrega de Pacotes de Aplicativos**.

> **Nota:**
>
> - O Microsoft App-V Desktop Client é o componente que executa aplicativos virtuais de pacotes App-V em dispositivos de usuário. O Windows 10 (1607 ou posterior) e o Windows Server 2019 e posterior já incluem este software cliente App-V. Você deve

habilitá-lo apenas em máquinas VDA. Para obter mais informações, consulte este artigo da documentação da Microsoft: Habilitar o cliente App-V integrado.

- Para aplicativos FlexApp, instale o FlexApp One Agent no VDA juntamente com o Componente de Entrega de Pacotes de Aplicativos.
- Para aplicativos Elastic App, instale a imagem habilitada para App Layering no VDA juntamente com o Componente de Entrega de Pacotes de Aplicativos.
- Para aplicativos Cloudpaging, instale o Cloudpaging Player no VDA juntamente com o Componente de Entrega de Pacotes de Aplicativos.

INSTALAR O FLEXAPP ONE AGENT

1. Inicie um prompt de comando de administrador no VDA.
2. Localize o caminho de rede para qualquer Pacote FlexApp One.
3. Insira o seguinte comando:

```
\\path\to\any\FlexAppOnePackage.exe --install
```

4. Aceite quaisquer prompts que apareçam.

INSTALAR A IMAGEM HABILITADA PARA APP LAYERING

1. Configure o App Layering. Siga as instruções na documentação do Citrix App Layering. O processo inclui:
   a. Configure o Enterprise Layer Manager (ELM).
   b. Importe uma imagem de SO dourada.
   c. Criar uma camada de plataforma.
   d. Criar camadas de aplicativo.
   e. No ELM, selecione a caixa de seleção **Habilitar esta Camada de Aplicativo para uso com Pacotes de Aplicativo do Studio** para cada camada de aplicativo que você deseja entregar.
2. Instale uma imagem que inclua o componente Elastic Layering nas máquinas VDA. Você pode usar uma das seguintes maneiras:
   a. Implante a imagem do ELM com o Elastic Layering habilitado.

b. Instale o VDA manualmente na máquina e selecione o componente Elastic Layering durante a configuração.

INSTALAR O CLOUDPAGING PLAYER

1. Abra um prompt de comando de administrador no VDA.
2. Vá para a pasta que contém o instalador do Cloudpaging Player.
3. Execute o seguinte comando para instalar o player silenciosamente e configurar a URL do console SaaS. Substitua os valores de espaço reservado conforme necessário:

```
cloudpaging-player-setup-x64-release.exe /S /v"/qn ADDLOCAL=ALL
REG_BASETOKENPATHORURL=https://your-tenant-url/api/token"
```

4. (Opcional) Verifique a configuração após a instalação, verificando o seguinte valor de registro:

   - **Caminho:** `HKEY_LOCAL_MACHINE\SOFTWARE\Numecent\StreamingCore\Settings\Launcher`
   - **Nome:** `BaseTokenPathOrURL`
   - **Dados:** O valor deve corresponder à URL que você especificou durante a instalação.

Entregar aplicativos empacotados

Depois de concluir a instalação dos pré-requisitos, faça o seguinte para entregar aplicativos empacotados aos seus usuários:

1. Armazenar pacotes de aplicativos em compartilhamentos de rede.
2. Carregar pacotes de aplicativos para o seu ambiente.
3. Adicionar aplicativos a grupos de entrega.
4. Para habilitar a entrega automática de pacotes App-V interdependentes, crie grupos de isolamento.

ARMAZENAR PACOTES DE APLICATIVOS EM COMPARTILHAMENTOS DE REDE

Depois de configurar a infraestrutura, gere os pacotes de aplicativos e armazene-os em um local de rede, como um compartilhamento de rede UNC ou SMB, ou em um Compartilhamento de Arquivos do Azure.

As etapas detalhadas são as seguintes:

1. Gere pacotes de aplicativos. Consulte a documentação da Microsoft: Criação e gerenciamento de aplicativos virtualizados App-V para obter detalhes.

2. Armazene pacotes de aplicativos em um local de rede:

    - Para **App-V Single Admin**: Armazene os pacotes e os arquivos de configuração dinâmica correspondentes (App-V) em um compartilhamento de rede UNC ou SMB ou em um Compartilhamento de Arquivos do Azure.
    - Para **App-V Dual Admin**: Publique os pacotes no servidor de gerenciamento App-V a partir de um caminho UNC. (A publicação a partir de URLs HTTP não é suportada.)
    - Para **MSIX ou MSIX app attach**: Armazene os pacotes em um compartilhamento de rede UNC ou SMB ou em um Compartilhamento de Arquivos do Azure.
    - Para **FlexApp**: Armazene os pacotes em um compartilhamento de rede UNC ou SMB ou em um Compartilhamento de Arquivos do Azure.
    - Para **Elastic App**: Armazene os pacotes em um compartilhamento de rede UNC ou SMB ou em um Compartilhamento de Arquivos do Azure.
    - Para **Cloudpaging**: Armazene os pacotes em um compartilhamento de rede UNC ou SMB ou em um Azure File Share.

3. Certifique-se de que o VDA tenha permissão de leitura no caminho de armazenamento do pacote:

    - Se você armazenar pacotes em um compartilhamento de rede UNC ou SMB em seu domínio AD, conceda à máquina VDA permissão de leitura para o caminho de armazenamento. Para fazer isso, você pode dar à conta AD da máquina permissão de leitura para o compartilhamento explicitamente, ou incluir a conta em um grupo AD que tenha essa permissão.
    - Se você armazenar pacotes em um Azure File Share, primeiro conceda a uma conta de usuário permissão de leitura para o caminho de armazenamento no Azure. Em seguida, configure `ctxAppVService` em execução na máquina VDA para usar essa conta de usuário para acessar o caminho de armazenamento do pacote. Consulte Alterar a conta de logon do usuário para obter as etapas detalhadas.

ALTERAR A CONTA DE LOGON DO USUÁRIO

Altere a conta de logon do usuário nos dois cenários a seguir:

- Para acessar pacotes em um Azure File Share usando uma conta AD vinculada:
    - A entidade de conexão deve ser uma conta de usuário, não uma conta de máquina, pois o Microsoft Entra ID não concede permissões de leitura a contas de máquina em File Shares.

- Se os pacotes MSIX e MSIX AppAttach contiverem serviços:
    - O pacote deve ser publicado usando uma conta de usuário com privilégios administrativos na máquina local antes que possa ser publicado para quaisquer usuários não administrativos. Isso é necessário para que os serviços empacotados sejam instalados e os pacotes só podem ser publicados para usuários, não para máquinas, tornando a conta LocalService padrão inadequada.

O VDA chama `ctxAppVService` para acessar caminhos de armazenamento de pacotes e executar operações que exigem privilégios administrativos. Por padrão, `ctxAppVService` é executado no contexto da conta LocalService da máquina que se autentica no AD usando a identidade da máquina e não é adequado para os cenários anteriores.

Em ambos os casos, o serviço deve ser reconfigurado para usar uma conta de usuário AD que tenha privilégios administrativos localmente e que tenha recebido acesso de leitura ao local de armazenamento dos pacotes, seja um compartilhamento SMB ou um Azure File Share, da seguinte forma:

1. Inicie **Serviços**, clique com o botão direito em **ctxAppVService** e selecione **Propriedades**.
2. Na guia **Fazer logon**, selecione **Esta conta**:
    a. Insira uma conta de usuário que tenha privilégios administrativos locais e permissão de leitura para o caminho de armazenamento do pacote
    b. Digite a senha do usuário duas vezes.
3. Clique em **OK**.

CARREGAR PACOTES DE APLICATIVOS PARA O SEU AMBIENTE

Depois de armazenar os pacotes de aplicativos em um local de rede conforme necessário, carregue-os para o seu ambiente para entrega. Use um dos seguintes métodos conforme necessário:

- Carregar em massa
- Carregar um por um

Preparações
O Citrix DaaS usa uma máquina VDA para configurar a conexão com o local de rede para descoberta de pacotes. Portanto, crie um grupo de entrega antecipadamente e certifique-se de que pelo menos um VDA no grupo atenda aos seguintes requisitos:

- Versão do VDA:

  - Para descobrir pacotes App-V: 2203 ou posterior
  - Para descobrir pacotes MSIX e MSIX app attach: 2209 ou posterior
  - Para descobrir pacotes FlexApp: 2311 ou posterior e o software FlexApp Agent
  - Para descobrir pacotes Elastic App: 2511 ou posterior e a imagem habilitada para App Layering
  - Para descobrir pacotes Cloudpaging do console Cloudpager: 2511 ou posterior
  - Para descobrir pacotes Cloudpaging de um compartilhamento de rede: 2603 ou posterior
- Componente de Entrega de Pacotes de Aplicativos: Instalado
- Permissão no local do pacote: Leitura (Consulte Armazenar pacotes de aplicativos em compartilhamentos de rede para obter detalhes.)
- Energia: Ligado
- Estado: Registrado

Carregar pacotes de aplicativos em massa
Carregue pacotes em um local de rede para o seu ambiente. Certifique-se de ter os seguintes itens prontos antes do carregamento:

- Um grupo de entrega que atenda aos requisitos de Preparações
- O caminho do local de rede

Para carregar pacotes em massa, siga estas etapas:

1. No painel esquerdo, selecione **Pacotes de aplicativos**.
2. Na guia **Descoberta de pacotes**, clique no botão **Criar perfil de descoberta**. A página **Criar perfil de descoberta** é exibida.
3. No campo **Nome**, insira um nome descritivo para o perfil.
4. No campo **Grupo de entrega**, clique em **Selecionar um grupo de entrega**. Em seguida, selecione um grupo de entrega que atenda aos requisitos indicados em Preparações e clique em **OK**.
5. No campo **Tipo de local**, selecione **Servidor Microsoft App-V**, **Compartilhamento de rede** ou **Numecent Cloudpager** com base em onde você armazena os pacotes, e, em seguida, conclua as configurações correspondentes:
   - Se você selecionou **Servidor Microsoft App-V**, insira as seguintes informações:
     - URL do servidor de Gerenciamento. Exemplo: `http://appv-server.example.com`

  - Credenciais de login do administrador do servidor de gerenciamento.
  - URL e número da porta do servidor de publicação. Exemplo: `http://appv-server.example.com:3330`

- Se você selecionou **Compartilhamento de rede**, especifique as seguintes informações:
  - Insira o caminho UNC do compartilhamento de rede (Exemplo: `\\Package-Server\apps\`). Para *pacotes Elastic App*, insira o caminho UNC do **System's Network File Share SMB path** no ELM.
  - Selecione os tipos de pacote que você deseja carregar. As opções incluem **App-V**, **MSIX**, **MSIX app attach**, **FlexApp**, **Elastic App** e **Cloudpaging**.
  - Especifique se deseja pesquisar subpastas por pacotes.

    > **Nota:**
    >
    > Se você pesquisar pacotes MSIX app attach em uma estrutura de pastas contendo imagens `cim`, certifique-se de selecionar **Pesquisar** subpastas. Caso contrário, os discos não serão descobertos corretamente.

- Se você selecionou **Numecent Cloudpager** (o que significa que os aplicativos Cloudpaging são armazenados no console Cloudpager), insira as seguintes informações:
  - URL do console Cloudpager. Exemplo: `https://cloudpagerconsole.my.org`
  - Chave da API do PowerShell.
  - MSID do AppLauncher.

6. Na seção **Preferências**, configure as seguintes opções conforme necessário:

- **Remover pacotes ausentes**: Selecione esta opção para remover automaticamente pacotes da guia **Pacotes** se eles não forem mais encontrados no local do perfil durante as verificações de atualização. Se não for selecionada, esses pacotes aparecerão com um ícone desabilitado.
- **Atualizar no local**: Selecione esta opção para sobrescrever um pacote existente com uma versão mais recente descoberta durante uma verificação de atualização. Quando selecionada, os favoritos do usuário são mantidos após a atualização. Esta opção é selecionada por padrão.

- **Ignorar downgrade**: Selecione esta opção para ignorar a importação de um pacote se uma versão superior do mesmo pacote já existir na biblioteca. Esta opção é selecionada por padrão.

7. Clique em **Criar perfil de descoberta**.

   A página **Criar perfil de descoberta** é fechada e o perfil recém-adicionado aparece na lista de perfis. O Citrix DaaS carrega os pacotes para o Citrix Cloud usando um VDA no grupo de entrega. Após a conclusão do upload, o campo Status mostra Importação bem-sucedida. Os pacotes correspondentes aparecem na guia **Pacotes**.

> **Nota:**
>
> - Para verificar atualizações de pacotes em um local de perfil e importá-los para o Citrix Cloud, selecione o local na lista de perfis e clique em **Verificar atualizações**.
> - Ao selecionar um perfil de descoberta na lista, o painel de detalhes mostra os valores atuais de **Atualizar no local** e **Ignorar downgrade** como **Sim** ou **Não**.
> - Ao clicar em **Verificar atualizações**, o painel de confirmação também exibe as configurações atuais de **Atualizar no local** e **Ignorar downgrade** antes que a verificação seja executada.

Carregar pacotes de aplicativos um por um

Carregue um pacote de aplicativo de um compartilhamento de rede para seu ambiente. Antes do upload, certifique-se de ter os seguintes itens prontos:

- Um grupo de entrega que atenda aos requisitos estabelecidos em Preparações
- O caminho do local de rede.

Para carregar um pacote para seu ambiente, siga estas etapas:

1. No painel esquerdo, selecione **Pacotes de aplicativos**.
2. Na guia **Pacotes**, clique no botão **Adicionar pacote**. A página **Adicionar pacote** é exibida.
3. No campo **Grupo de entrega**, clique em **Selecionar um grupo de entrega**. Em seguida, selecione um grupo de entrega que atenda aos requisitos indicados em Preparações e clique em **OK**.
4. No campo **Caminho completo do pacote**, insira um caminho conforme necessário:

- Para carregar vários pacotes de uma vez, insira seus caminhos completos, separados por ponto e vírgula (`;`). Exemplo: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
- Para carregar todos os pacotes presentes em um compartilhamento de rede, insira o caminho de armazenamento. Exemplo: `\\package-Server\apps\`

5. Na seção **Preferências**, configure as seguintes opções conforme necessário:
   - **Atualizar no local**: Selecione esta opção para sobrescrever um pacote existente com uma versão mais recente quando uma for encontrada. Quando selecionada, os favoritos do usuário são mantidos após a atualização. Esta opção é selecionada por padrão.
   - **Ignorar downgrade**: Selecione esta opção para pular a importação deste pacote se uma versão superior do mesmo pacote já existir na biblioteca. Esta opção é selecionada por padrão.
6. Clique em **Adicionar Pacote**.

   O pacote de aplicativos aparece na guia **Pacotes**.

ADICIONAR APLICATIVOS A GRUPOS DE ENTREGA

Depois que um pacote de aplicativos é totalmente carregado em seu ambiente, adicione seus aplicativos a um ou mais grupos de entrega conforme necessário. Como resultado, os usuários associados a esses grupos de entrega podem acessar os aplicativos.

> **Nota:**
>
> - Você pode entregar aplicativos empacotados para VDAs de sessão única e VDAs de múltiplas sessões por meio de grupos de entrega.
> - Por padrão, os usuários finais têm acesso a todos os aplicativos empacotados atribuídos aos grupos de entrega associados aos seus VDAs de *sessão única* (ou chamados de *Desktop*). Para limitar a visibilidade de um aplicativo empacotado em VDAs de *desktop* a usuários ou grupos específicos, vá para o nó **Aplicativos**, selecione o aplicativo e, em seguida, selecione **Editar Propriedades do Aplicativo > Limitar Visibilidade** para fazer alterações. Consulte Limitar visibilidade de aplicativos

> Para adicionar um ou mais aplicativos em um pacote a vários grupos de entrega, siga estas etapas:

1. No painel esquerdo, selecione **Pacotes de Aplicativos**.
2. Na guia **Pacotes**, selecione um pacote conforme necessário.
3. Na barra de ações, clique em **Adicionar Grupos de Entrega**. A página **Atribuir Aplicativos a Grupos de Entrega** é exibida.
4. Selecione onde entregar aplicativos deste pacote de aplicativos, selecione um ou mais aplicativos no pacote para o aplicativo Citrix Workspace e, em seguida, clique em **Avançar**.

    - **Entregar o pacote de aplicativos na área de trabalho**: Todos os aplicativos neste pacote são entregues em áreas de trabalho virtuais Citrix. Os usuários finais podem acessá-los iniciando uma área de trabalho na guia **Áreas de Trabalho** de sua loja.
    - **Entregar os aplicativos no Citrix Workspace**: Os aplicativos selecionados neste pacote são entregues como aplicativos virtuais Citrix. Os usuários finais podem acessá-los na guia **Aplicativos** de sua loja.

    > **Nota:**
    >
    > Essa configuração controla a visibilidade padrão dos aplicativos empacotados. Para alterar a visibilidade de um aplicativo empacotado específico posteriormente, vá para o nó **Aplicativos**, selecione o aplicativo e escolha **Propriedades > Entrega** para fazer as alterações. Para obter mais informações, consulte Alterar propriedades do aplicativo.

5. Na lista de grupos de entrega, selecione os grupos aos quais você deseja atribuir os aplicativos e, em seguida, clique em **Avançar**.

    > **Nota:**
    >
    > - Se você selecionou um pacote MSIX ou MSIX app attach, somente os grupos de entrega cuja versão do VDA seja 2106 ou posterior serão exibidos na lista.
    > - Se você selecionou um pacote *FlexApp*, somente os grupos de entrega cuja versão do VDA seja 2402 ou posterior aparecerão na lista.
    > - Se você selecionou um pacote *Elastic App*, somente os grupos de entrega cuja versão do VDA seja 2511 ou posterior aparecerão na lista.
    > - Se você selecionou um pacote *Cloudpaging*, somente os grupos de entrega cuja versão do VDA seja 2511 ou posterior aparecerão na lista.

6. Clique em **Concluir**.

Para adicionar aplicativos em vários pacotes a múltiplos grupos de entrega, siga estas etapas:

1. No painel esquerdo, selecione **Pacotes de Aplicativos**.
2. Na guia **Aplicativos**, selecione **Adicionar Aplicativos**.
3. Na página **Grupos**, selecione um ou mais grupos de entrega conforme necessário.
4. Na página **Aplicativos**, selecione um ou mais pacotes de aplicativos da seguinte forma:
    a. Clique em **Adicionar** e, em seguida, selecione **Pacotes de aplicativos**.
    b. Selecione o tipo de pacote necessário (por exemplo, App-V Single Admin). Todos os pacotes deste tipo aparecerão.
    c. Selecione um ou mais pacotes conforme necessário.
    d. Clique em **OK** e, em seguida, em **Avançar**.
    e. Para adicionar mais aplicativos de um tipo de pacote diferente, repita as etapas de 'a' a 'd'.
5. Clique em **Concluir**.

Você também pode adicionar aplicativos empacotados a um grupo de entrega quando:

- Criar um grupo de entrega. Para obter mais informações, consulte Criar grupos de entrega.
- Editar grupos de entrega ou grupos de aplicativos existentes. Para obter mais informações, consulte Adicionar aplicativos.

(OPCIONAL) CRIAR GRUPOS DE ISOLAMENTO PARA PACOTES APP-V

Você pode criar grupos de isolamento para permitir a entrega automática de pacotes App-V interdependentes.

> **Nota:**
>
> Os grupos de isolamento são suportados para o método App-V Single Admin. Se você estiver usando o método App-V Dual Admin, poderá atingir o mesmo objetivo criando *grupos de conexão* na infraestrutura do Microsoft App-V. Para obter mais informações, consulte este artigo da documentação da Microsoft: Sobre o arquivo do grupo de conexão.

Sobre grupos de isolamento

Um grupo de isolamento é uma coleção de pacotes de aplicativos interdependentes que devem ser executados na mesma Windows Sandbox para criar um ambiente virtual. Os grupos de isolamento do Citrix App-V são semelhantes, mas não idênticos, aos grupos de conexão do App-V. Um grupo de isolamento inclui dois tipos de pacotes:

- **Pacotes de aplicativos explícitos**: Aplicativos com requisitos de licenciamento específicos. Você pode restringir esses aplicativos a um intervalo específico de usuários adicionando-os a grupos de entrega.
- **Pacotes de aplicativos automáticos**: Aplicativos que estão sempre disponíveis para todos os usuários, independentemente de serem adicionados a grupos de entrega.

Por exemplo, o aplicativo `app-a` requer JRE 1.7 para ser executado. Você pode criar um grupo de isolamento que contenha app-a (marcado como *Explícito*) e JRE 1.7 (marcado como *Automático*). Em seguida, adicione o pacote App-V para `app-a` a um ou mais grupos de entrega. Quando um usuário inicia o app-a, o JRE 1.7 é implantado automaticamente com ele.

Quando um usuário inicia um aplicativo App-V marcado como *Explícito* em um grupo de isolamento, o Citrix DaaS verifica a permissão de acesso do usuário ao aplicativo nos grupos de entrega. Se o usuário tiver permissão para acessar o aplicativo, quaisquer pacotes de aplicativos *Automáticos* no mesmo grupo de isolamento serão disponibilizados ao usuário.

Você não precisa adicionar os pacotes *Automáticos* a nenhum grupo de entrega. Se houver outro pacote de aplicativo *Explícito* no grupo de isolamento, esse pacote será disponibilizado ao usuário somente se estiver no mesmo grupo de entrega.
Criar um grupo de isolamento App-V
Crie um grupo de isolamento e adicione pacotes de aplicativos interdependentes a ele. As etapas detalhadas são as seguintes:

1. Na guia **Grupos de Isolamento**, clique em **Adicionar Grupo de Isolamento**.
2. Insira um nome e uma descrição para o grupo de isolamento. Todos os pacotes App-V Single Admin em seu ambiente aparecem na lista **Pacotes Disponíveis**.
3. Na lista **Pacotes Disponíveis**, selecione um aplicativo conforme necessário e clique na seta para a direita. O aplicativo selecionado aparece na lista **Pacotes no Grupo de Isolamento**.
4. No campo **Implantação**, selecione **Explícito** ou **Automático** para o aplicativo.
5. Repita os passos 2–3 para adicionar mais pacotes.
6. Para ajustar a ordem dos pacotes na lista, clique na seta para cima ou para baixo.
7. Clique em **Salvar**.

> **Nota:**

> As configurações do Grupo de Isolamento resultam na criação de Grupos de Conexão App-V no VDA. Os cenários de implantação podem se tornar complexos e o cliente App-V suporta pacotes que estão em apenas um Grupo de Conexão ativo por vez. Recomendamos que você evite adicionar o mesmo pacote a dois grupos de isolamento diferentes que são adicionados ao mesmo grupo de entrega.

Melhores práticas

- Para implantar pacotes App-V, habilite o subsistema App-V no VDA usando o comando PowerShell `Enable-AppV`.
- Para implantar pacotes MSIX (e AppAttach), o VDA deve confiar nos certificados com os quais os pacotes são assinados.
- No Windows Server 2019, habilite o sideloading para implantar pacotes MSIX. O sideloading não é necessário para Windows 10, 11, Windows Server 2022 e 2025.
- O App Attach não tem implementação alguma no Windows Server 2019 e não é atualmente suportado pela Microsoft (ou pela Citrix, por extensão) no Windows Server 2022 ou 2025.

Avançado

Os seguintes tópicos avançados fornecem opções e controles de configuração adicionais para ajustar como os aplicativos empacotados são descobertos, atualizados e entregues no Citrix DaaS, além do fluxo de trabalho básico de pacotes de aplicativos.

Automatizar a publicação de aplicativos empacotados

Você pode usar comandos PowerShell para automatizar a publicação de aplicativos empacotados:

No Delivery Controller™, execute os seguintes comandos PowerShell:

1. Para carregar os comandos presentes no Módulo de Descoberta de Pacotes:

```
Import-Module "D:
\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

> **Nota:**

> A versão do módulo de descoberta de pacotes pode ser encontrada na ISO do Citrix DaaS no caminho mencionado na etapa 1.

2. O módulo de descoberta de pacotes deve ser da ISO de uma versão do Citrix DaaS que também suporte o tipo de pacote que você está publicando, ou seja, 2311 ou superior é necessário para Aplicativos FlexAppOne. Recomendamos usar a versão mais recente disponível.
3. Para recuperar os IDs de grupo de entrega e os IDs de aplicativos empacotados relevantes:

```
Get-BrokerDesktopGroup | Format-Table Uid, Name

Get-AppLibAppVApplication | Format-Table Uid, Name
```

4. Para publicar os pacotes e criar as BrokerMachineConfigurations apropriadas:

```
Publish-PackagedApplication -AppLibararyApplicationUid
<AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
```

5. Para sincronizar as configurações do Broker, que são posteriormente enviadas para o agente Broker no VDA:

```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid
<DesktopGroup.Uid>
```

> **Nota:**
>
> Certifique-se de executar o comando PowerShell `Update-DesktopGroupMachineConfigurations` depois de publicar ou remover aplicativos empacotados de um grupo de entrega por meio da linha de comando do PowerShell. Caso contrário, as informações sobre os aplicativos publicados não são enviadas corretamente para o VDA e os lançamentos falham.

Limitar a visibilidade de aplicativos

Em um ambiente Citrix DaaS, quando aplicativos de pacotes são publicados em desktops, o sistema respeita as configurações de visibilidade de usuário e grupo do Active Directory (AD) para esses aplicativos. No entanto, mesmo que um usuário tenha visibilidade apenas para um

aplicativo dentro de um pacote, o pacote inteiro deve ser implantado na Sessão de Área de Trabalho Virtual (ou Aplicativo Seamless), pois os componentes individuais do pacote não podem ser subdivididos no VDA. Além disso, antes da versão 2503 do VDA, as alterações que reduzem a visibilidade do aplicativo após a publicação inicial não resultarão em uma limpeza de pacotes publicados anteriormente em lançamentos de desktop subsequentes. Além disso, outras camadas de visibilidade, como visibilidade de desktop versus workspace, operam sobre essas atribuições de visibilidade do AD.

Você pode controlar se os aplicativos empacotados devem aparecer no Workspace ou são implantados nas sessões de Desktop VDI dos usuários. Depois que um aplicativo empacotado for publicado, você pode atualizar a propriedade `PackagedApplicationVisibility` no `BrokerApplictaion` usando o comando PowerShell `Set-BrokerApplication -Name "MyApp" -PackagedApplicationVisibility "Workspace|Desktop|WorkspaceAndDesktop"`.

O valor padrão de `PackagedApplicationVisibility` é `WorkspaceAndDesktop`.

O valor `Workspace`: o aplicativo aparece apenas no WorkspaceApp e está disponível para um AppLaunch contínuo, mas o aplicativo não será publicado automaticamente em nenhuma sessão de desktop que os usuários iniciarem.

O valor `Desktop`: oculta o ícone do aplicativo do WorkspaceApp, tornando-o indisponível para um AppLaunch contínuo, mas o aplicativo ainda pode ser implantado nas sessões de desktop dos usuários se eles também tiverem acesso a ele por meio de suas configurações de Grupo AD.

> **Nota:**
>
> Aplicativos Empacotados publicados em desktops Estáticos de Sessão Única nunca estão disponíveis no Workspace App, independentemente do valor configurado nesta configuração.

Migrar da infraestrutura completa do App-V para o fluxo de trabalho de Administrador Único

A infraestrutura completa do Microsoft App-V (Administrador Duplo) está se aproximando do fim da vida útil. Para continuar entregando pacotes App-V e outros formatos de contêiner suportados, migre para o modelo de Administrador Único da Citrix.

O modelo de Administrador Único remove a dependência dos servidores de Gerenciamento e Publicação do App-V e centraliza o gerenciamento de pacotes no Studio.

Benefícios do modelo de Administrador Único

A mudança para o fluxo de trabalho de Administrador Único simplifica sua arquitetura e otimiza o gerenciamento de pacotes.

ARQUITETURA SIMPLIFICADA

No modelo de Administrador Único, o VDA recupera pacotes diretamente do compartilhamento de arquivos. A Citrix gerencia metadados, publicação e lógica de isolamento.

RECURSO	INFRAESTRUTURA COMPLETA (ADMINISTRADOR DUPLO)	ADMINISTRADOR ÚNICO (GERENCIADO PELA CITRIX)
Gerenciamento	Console de Gerenciamento do App-V	Citrix Studio ou Web Studio
Banco de dados	Obrigatório (SQL Server)	Nenhum (metadados armazenados no banco de dados do site Citrix)
Publicação	Servidor de Publicação App-V	Citrix VDA (`ctxAppVService`)
Origem do pacote	Compartilhamento UNC (sincronizado com o Servidor de Gerenciamento)	Compartilhamento UNC, compartilhamento SMB ou Azure Files
Lógica	Grupos de Conexão	Grupos de Isolamento Citrix

VANTAGEM ESTRATÉGICA

Ao migrar para o Single Admin, você também elimina o **Atraso de Sincronização**.

- No modelo de Administrador Duplo, você deve sincronizar o Servidor de Gerenciamento App-V e, em seguida, sincronizar o Studio.
- No modelo de Administrador Único, ao atualizar um pacote no compartilhamento de arquivos e selecionar **Atualizar** no Studio, o pacote atualizado estará disponível no próximo logon do usuário.

Fluxo de trabalho de migração

Siga estas etapas para mover sua infraestrutura App-V completa existente para o fluxo de trabalho de Administrador Único da Citrix:

1. Etapa 1: Preparar o ambiente de destino
2. Etapa 2: Importar pacotes para a biblioteca Citrix

ETAPA 1: PREPARAR O AMBIENTE DE DESTINO

Antes de importar pacotes, certifique-se de que sua infraestrutura e VDAs estejam prontos para suportar o modelo de Administrador Único.

1. **Repositório compartilhado**
   a. Identifique o compartilhamento UNC que hospeda seus pacotes `.appv`.
   b. Certifique-se de que as contas de máquina VDA (por exemplo, Computadores de Domínio) tenham acesso de **Leitura** tanto ao compartilhamento quanto às permissões NTFS.
2. **VDAs**

   Certifique-se de que todos os VDAs tenham o **Componente de Entrega de Pacotes de Aplicativos** instalado. Para adicionar este componente após a instalação:

   a. Execute o instalador do VDA.
   b. Selecione **Alterar** em **Programas e Recursos**.
   c. Adicionar **Componente de Entrega de Pacotes de Aplicativos**.
3. **Arquivos de configuração XML**

   Mova os arquivos `_DeploymentConfig.xml` e `_UserConfig.xml` para a *mesma* pasta que o arquivo `.appv` correspondente.

   No modelo de Administrador Único, o VDA lê os arquivos de configuração da pasta do pacote no compartilhamento de arquivos, em vez de um banco de dados App-V central.

ETAPA 2: IMPORTAR PACOTES PARA A BIBLIOTECA CITRIX

Depois de preparar o ambiente, importe seus pacotes App-V existentes para a biblioteca de aplicativos Citrix.

1. No Citrix Studio, vá para **Configuração** > **Pacotes de Aplicativos**.
2. Se você estiver migrando totalmente, remova todas as conexões existentes com o Servidor de Gerenciamento App-V.
3. Selecione **Adicionar Pacote** e aponte-o para o caminho UNC do seu pacote.
4. O Citrix verifica a pasta e importa nomes de pacotes, versões e IDs de aplicativos para a biblioteca de aplicativos Citrix.

Após a importação, você pode atribuir aplicativos a grupos de entrega conforme necessário.

Nota:

Política vPrefer (Opcional): Se você quiser que os aplicativos sejam iniciados no VDA local em vez de serem redirecionados para um servidor remoto, ative o GPO **vPrefer** em seus VDAs.

Solucionar problemas de aplicativos App-V (modelo de Administrador Único)

Se os pacotes App-V (no modelo de Administrador Único) não forem iniciados ou não aparecerem na sessão do usuário, use as seguintes orientações para identificar e resolver problemas comuns.

PROBLEMA	DESCRIÇÃO	SOLUÇÃO
Descoberta de pacote e erros de "Falha ao catalogar"	Ao adicionar um pacote no Studio, um erro indica que o arquivo não pode ser acessado ou que os metadados são inválidos.	1. Verifique as permissões. Certifique-se de que a conta de máquina do Delivery Controller (por exemplo, `DOMAIN\DDC01$`) tenha permissões de **Leitura** nos níveis de compartilhamento e NTFS do caminho UNC que hospeda o pacote. 2. Verifique a integridade do XML.

PROBLEMA	DESCRIÇÃO	SOLUÇÃO
		Certifique-se de que o arquivo `.appv` e o arquivo `_DeploymentConfig.xml` tenham o mesmo prefixo de nome de arquivo e estejam localizados na mesma pasta.
O aplicativo falha ao iniciar (código de erro: 0x80070005 ou 0x80040154)	O usuário clica no ícone do aplicativo e a tela de **inicialização do Citrix** aparece, mas o aplicativo não abre.	1. Verifique o componente VDA. Certifique-se de que o **Componente de Entrega de Pacotes de Aplicativos** esteja instalado no VDA. Confirme se o seguinte arquivo existe: `C:\Program Files\Citrix\AppV\ctxAppVService.exe`.

PROBLEMA	DESCRIÇÃO	SOLUÇÃO
		2. Verifique as permissões do VDA. Como o VDA extrai o pacote do compartilhamento de arquivos, a conta de máquina do VDA (por exemplo, `DOMAIN\VDA-HR01$`) deve ter acesso de **Leitura** ao caminho UNC. 3. Valide a configuração do cliente App-V. • Execute o seguinte comando PowerShell no VDA: `Get-AppvClientConfiguration`. • Se o seu pacote requer scripts, certifique-se de que `EnablePackageScripts` está

PROBLEMA	DESCRIÇÃO	SOLUÇÃO
		definido como `$True`.
Conflitos de grupo de isolamento	Um plug-in, como um suplemento do Excel, não consegue ver sua aplicação pai.	1. No Studio, vá para **Pacotes de Aplicativos** > **Grupos de Isolamento**. 2. Certifique-se de que ambos os pacotes sejam adicionados ao mesmo grupo de isolamento. No modelo de Administrador Único, o cliente App-V no VDA gerencia a conexão virtual dessas aplicações com base na configuração entregue pelo Delivery Controller.
Lançamento inicial lento (buffer)	O primeiro lançamento de um pacote App-V grande, como AutoCAD ou ArcGIS, leva vários minutos.	1. No VDA, verifique o seguinte registro:

PROBLEMA	DESCRIÇÃO	SOLUÇÃO
		`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AppV\Client\Streaming` 2. Defina `Autoload` como `2` (carregar automaticamente todos os pacotes usados anteriormente) para melhorar o desempenho de lançamento subsequente. 3. Verifique o desempenho da rede. Certifique-se de que a assinatura SMB ou a verificação antivírus no compartilhamento de rede não esteja limitando a velocidade de transferência.

Comandos úteis do PowerShell (executados no VDA)

Para verificar se o Citrix entregou o pacote com sucesso ao VDA, execute os seguintes comandos em uma janela do PowerShell:

COMANDO	PROPÓSITO
`Get-AppvClientPackage`	Exibe todos os pacotes App-V atualmente armazenados em cache ou publicados no VDA.
`Get-CtxAppvPackage`	Exibe os pacotes gerenciados pelo agente Citrix.
`Start-Service ctxAppVService`	Reinicia o serviço de orquestração do Citrix App-V.

Autoscale™

O Autoscale oferece uma solução consistente e de alto desempenho para gerenciar proativamente o consumo de energia de suas máquinas. Seu objetivo é equilibrar custos e experiência do usuário. O Autoscale incorpora a tecnologia Smart Scale descontinuada na solução de gerenciamento de energia do Studio.

O Autoscale permite o gerenciamento proativo de energia de todas as máquinas OS de sessão única e multissessão registradas em um grupo de entrega.

Os recursos do Autoscale incluem:

- Configurações baseadas em agendamento e em carga
- Tempos limite de sessão dinâmicos
- Máquinas marcadas pelo Autoscale (burst de nuvem)
- Provisionamento dinâmico de máquinas
- Notificações de logoff do usuário

Casos de uso típicos

A seguir estão os cenários onde o AutoScale é comumente usado.

- Ligar máquinas com base em agendamento para manipular a carga de trabalho esperada

  O Autoscale permite que os administradores variem a capacidade ligada com granularidade de 30 minutos e permite agendamentos diferentes em dias diferentes. Se uma carga de trabalho volátil for esperada, é aconselhável configurar o buffer de capacidade para evitar que os usuários tenham que esperar as máquinas ligarem.

- Caso de uso de burst de nuvem

  O Autoscale oferece a flexibilidade para gerenciar a energia de apenas um subconjunto de máquinas em um grupo de entrega. Para conseguir isso, aplique uma tag a uma ou mais máquinas e então configure o Autoscale para gerenciar a energia apenas das máquinas marcadas.

  Este recurso pode ser útil em casos de uso de cloud bursting, onde você deseja usar recursos locais (ou instâncias de nuvem pública reservadas) para manipular cargas de trabalho antes que os recursos baseados em nuvem atendam à demanda adicional (ou seja, cargas de trabalho de pico).

- Usuários com aumento gradual ou usuários sazonais

  Quando uma organização tem usuários sendo integrados lentamente e não deseja provisionar toda a capacidade antecipadamente, o recurso de provisionamento dinâmico pode ajudar. O recurso avalia constantemente a carga no grupo de entrega e dimensiona dinamicamente para cima ou para baixo o número de máquinas no grupo de entrega com base nas condições de carga atuais. Um administrador deve definir os limites superior e inferior (watermark) para a carga no grupo de entrega para criar máquinas. Os administradores podem, opcionalmente, definir o número máximo de máquinas a serem provisionadas e as tags a serem aplicadas a essas máquinas.

Plataformas de hospedagem de VDA suportadas

O Autoscale suporta todas as plataformas que o Citrix DaaS suporta. Isso inclui várias plataformas de infraestrutura, como XenServer (anteriormente Citrix Hypervisor), AWS, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere e muitas outras. Para uma lista completa de plataformas suportadas, consulte Requisitos do sistema para Citrix DaaS.

Cargas de trabalho suportadas

O Autoscale suporta grupos de entrega de SO multi-sessão e SO de sessão única. Existem três interfaces de usuário a serem consideradas:

- Interface de usuário do Autoscale para grupos de entrega de SO multi-sessão (anteriormente grupos de entrega RDS)
- Interface de usuário do Autoscale para grupos de entrega de SO de sessão única aleatórios (agrupados) (anteriormente grupos de entrega VDI agrupados)
- Interface de usuário do Autoscale para grupos de entrega de SO de sessão única estáticos (anteriormente grupos de entrega VDI estáticos)

Para obter mais informações sobre as interfaces de usuário para diferentes grupos de entrega, consulte Interfaces de usuário do Autoscale.

Benefícios

O recurso Autoscale oferece os seguintes benefícios:

- Fornecer um mecanismo único e consistente para gerenciar o consumo de energia das máquinas em um grupo de entrega.
- Garantir a disponibilidade e controlar os custos, ligando as máquinas com gerenciamento de energia baseado em carga ou baseado em agendamento, ou uma combinação de ambos.
- Para monitorar métricas como economia de custos e utilização da capacidade, e para habilitar notificações, use o Director, disponível no console **Monitor**.

Assista a um vídeo de 2 minutos

O vídeo a seguir oferece um tour rápido pelo Autoscale.

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Introdução ao Autoscale™

Autoscale é um recurso que fornece uma solução consistente e de alto desempenho para gerenciamento de energia, a fim de escalar proativamente grupos de entrega com base em um agendamento configurado ou demandas de carga.

Autoscale aplica-se a todos os tipos de grupos de entrega:

- SO estático de sessão única
- SO aleatório de sessão única
- SO aleatório de múltiplas sessões

Este artigo descreve conceitos básicos relacionados ao Autoscale e fornece orientação sobre como habilitar e configurar o Autoscale para um grupo de entrega.

Conceitos básicos

Antes de começar, saiba mais sobre os seguintes conceitos básicos no Autoscale:

- Capacidade e registro de máquina
- Escala em vários catálogos de máquinas

- Provisionamento de máquina e demanda de sessão
- Considerações sobre o tamanho da instância
- Agendamentos
- Horários de pico e fora de pico
- Atraso de desligamento
- Tamanho do pool
- Buffer de capacidade
- Índice de carga
- Autoscale e modo de manutenção
- Custo da máquina
- Aumentar a escala de um grupo de entrega
- Diminuir a escala de um Grupo de Entrega
- Estado de drenagem

Capacidade e registro de máquinas

O Autoscale inclui apenas máquinas que estão registradas no site ao determinar a capacidade. Máquinas ligadas que não estão registradas não podem aceitar solicitações de sessão. Como resultado, elas não são incluídas na capacidade geral do grupo de entrega.

Escala em vários catálogos de máquinas

Em alguns sites, vários catálogos de máquinas podem estar associados a um único grupo de entrega. O Autoscale liga máquinas aleatoriamente de cada catálogo para atender aos requisitos de agendamento ou demanda de sessão.

Por exemplo, um grupo de entrega tem dois catálogos de máquinas: o Catálogo A tem três máquinas ligadas e o Catálogo B tem uma máquina ligada. Se o Autoscale precisar ligar uma máquina extra, ele poderá ligar uma máquina do Catálogo A ou do Catálogo B.

Provisionamento de máquinas e demanda de sessão

O catálogo de máquinas associado ao grupo de entrega deve ter máquinas suficientes para ligar e desligar conforme a demanda aumenta e diminui. Se a demanda de sessão exceder o número total de máquinas registradas no grupo de entrega, o Autoscale garante que todas as máquinas registradas sejam ligadas. No entanto, **o Autoscale não provisiona máquinas adicionais**.

> **Nota:**

Se um Grupo de Entrega tiver 63 máquinas e uma capacidade de buffer de 10% for definida para horários fora do expediente, então, de acordo com o cálculo do Autoscale, 6,3 máquinas devem ser ligadas durante os horários fora do expediente. Para manipular o valor decimal, as seguintes são as regras:

- Arredondar para o mais próximo: Por exemplo, se o valor for 6,4, então 6 máquinas são ligadas. Se o valor for 6,7, então 7 máquinas são ligadas.
- Arredondar para 1 para qualquer valor não zero menor que 1. Por exemplo, se o valor for 0,2 ou 0,9, então 1 máquina é ligada.

Para superar esse gargalo, você pode usar um script PowerShell para criar e excluir máquinas dinamicamente. Para mais informações, consulte Provisionar máquinas dinamicamente

Considerações sobre o tamanho da instância

Você pode otimizar seus custos se dimensionar adequadamente suas instâncias em nuvens públicas. Recomendamos que você provisione instâncias menores, desde que elas correspondam ao desempenho da sua carga de trabalho e aos requisitos de capacidade.

Instâncias menores hospedam menos sessões de usuário do que instâncias maiores. Portanto, o Autoscale coloca as máquinas em estado de drenagem mais rapidamente porque leva menos tempo para a última sessão de usuário ser desconectada. Como resultado, o Autoscale desliga instâncias menores mais cedo, o que reduz os custos.

Agendamentos

O Autoscale liga e desliga máquinas em um grupo de entrega com base em um agendamento que você define.

Um agendamento inclui o número de máquinas ativas para cada slot de tempo, com horários de pico e fora de pico definidos.

As configurações de agendamento variam com o tipo de grupo de entrega. Para mais informações, consulte:

- Grupos de entrega de SO multi-sessão
- Grupos de entrega aleatórios de SO de sessão única

- Grupos de entrega estáticos de SO de sessão única

Horários de pico e fora de pico

Horários de pico e fora de pico são usados para indicar quais dos valores de buffer de capacidade usar para períodos específicos do dia. Você pode definir os horários de pico, deixando os horários restantes não definidos como horários fora de pico.

Atraso de desligamento

O atraso de desligamento é o número mínimo de minutos que devem decorrer depois que uma máquina é ligada antes que o Autoscale possa desligá-la. Isso evita que as máquinas liguem e desliguem repetidamente durante demandas de sessão voláteis. Por padrão, o atraso de desligamento é de 30 minutos. Você pode configurá-lo em um intervalo de 0 a 60 minutos.

Tamanho do pool

O tamanho do pool é o número de máquinas que devem ser mantidas ligadas por um período específico do dia.

Buffer de capacidade

O buffer de capacidade é usado para adicionar capacidade sobressalente à demanda atual para contabilizar aumentos dinâmicos de carga. Existem dois cenários a serem observados:

- Para grupos de entrega de SO de várias sessões, o buffer de capacidade é definido como uma porcentagem da capacidade total do grupo de entrega em termos de índice de carga.
- Para grupos de entrega de SO de sessão única, o buffer de capacidade é definido como uma porcentagem do número total de máquinas no grupo de entrega.

O buffer de capacidade é um buffer contínuo, dado que é calculado e aplicado com base no uso atual, em vez de ser calculado e aplicado sobre o tamanho do pool configurado.

Por exemplo, dado um grupo de entrega com 10 máquinas, um tamanho de pool de 1 máquina para o período atual e um buffer de capacidade de 10%. Uma máquina adicional é ligada quando a 1 máquina ligada, conforme definido pelo agendamento, é carregada a ponto de o buffer de capacidade de 10% não ser mais satisfeito. Se a carga for reduzida após ligar a segunda máquina e houver capacidade de carga livre mais do que suficiente para satisfazer o buffer de capacidade de 10%, o Autoscale prepara 1 máquina para desligamento.

Índice de carga

> **IMPORTANTE:**

> O índice de carga se aplica apenas a grupos de entrega de várias sessões.

> A métrica do índice de carga determina a probabilidade de uma máquina receber solicitações de logon de usuário. Ela é calculada usando as configurações da **política de Gerenciamento de Carga do Citrix** configuradas para logon simultâneo, sessão, CPU, disco e uso de memória.

O índice de carga varia de 0 a 10.000. Por padrão, uma máquina é considerada em carga total quando hospeda 250 sessões:

- O dígito "0" indica uma máquina descarregada. Uma máquina com um valor de índice de carga de 0 está em uma carga de linha de base.
- O dígito "10.000" indica uma máquina totalmente carregada que não pode executar mais sessões.

Autoscale e modo de manutenção

Máquinas em modo de manutenção, independentemente do seu status de disponibilidade, são consideradas parte do cálculo do tamanho total do pool. Portanto, é possível que todas as máquinas dentro do pool estejam em modo de manutenção. No entanto, essas máquinas são excluídas dos cálculos do buffer de capacidade, garantindo sua disponibilidade imediata. Para garantir que uma porcentagem específica de máquinas esteja acessível para conexões de usuário, ajuste o tamanho do pool e os valores do buffer de acordo.

Custo da máquina

O custo da instância da máquina por hora é o custo por hora, em US$, da capacidade de computação sendo usada. Essa configuração é usada para calcular a economia de custos das configurações do Autoscale. Para visualizar a economia, vá para **Monitorar > Otimização de Custos > Economia de custos**.

Dimensionar um grupo de entrega

O Autoscale liga máquinas adicionais em um grupo de entrega habilitado para Autoscale quando:

1. O agendamento do Autoscale para o grupo de entrega indica que mais máquinas devem ser ligadas para o período atual.
2. A carga atual no grupo de entrega excedeu o buffer de capacidade.

Condições para ligar máquinas:

1. Não está em modo de manutenção.

2. O hipervisor não está em modo de manutenção.
3. Desligado e não registrado.
4. Pertence ao grupo de entrega que requer escalonamento vertical
5. Nenhuma ação de energia pendente.

Reduzir um grupo de entrega

O Autoscale desliga as máquinas em um grupo de entrega habilitado para Autoscale quando:

1. O agendamento do Autoscale especifica que as máquinas devem ser desligadas para atender ao número configurado de máquinas para o período atual.
2. A carga atual do grupo de entrega diminuiu, resultando em mais máquinas ligadas do que o necessário para atender ao tamanho do pool e ao buffer de capacidade.

O Autoscale reduz um grupo de entrega desligando as máquinas em excesso que excedem o número necessário para atender ao tamanho do pool e ao buffer de capacidade.

O processo de redução envolve duas etapas:

1. Coloque o número necessário de máquinas no estado de drenagem.
2. Selecione todas as máquinas drenadas para desligamento.

As máquinas elegíveis para desligamento devem atender aos seguintes critérios:

1. Não está em modo de manutenção
2. Hipervisor não está em modo de manutenção
3. Atualmente ligado
4. Registrado como disponível ou aguardando registro após a inicialização
5. Esgotado e sem sessões ativas
6. Nenhuma ação de energia pendente
7. Satisfaz o atraso de desligamento

Estado de drenagem

O Autoscale tenta reduzir o número de máquinas ligadas no grupo de entrega para o tamanho do pool configurado e o buffer de capacidade.

Para atingir esse objetivo, o Autoscale coloca as máquinas em excesso com o menor número de sessões em "estado de drenagem" e as desliga quando todas as sessões são encerradas. Esse

comportamento ocorre quando a demanda por sessões diminui e o agendamento exige menos máquinas do que as que estão ligadas.

Condições para que as máquinas entrem em estado de drenagem:

1. Ligado
2. Não estar em modo de manutenção
3. Hypervisor não em modo de manutenção
4. Pertence ao grupo de entrega que requer redução de escala
5. Menor número de sessões ativas atuais

Nota:

- Máquinas que estiveram ligadas por pelo menos o tempo especificado pelo atraso de desligamento são preferidas para drenagem.
- Máquinas em estado de drenagem não hospedam mais novos inícios de sessão e aguardam que as sessões existentes sejam encerradas. Uma máquina é desligada somente quando todas as sessões são encerradas. No entanto, se não houver máquinas imediatamente disponíveis para inícios de sessão, o Autoscale prefere direcionar os inícios de sessão para uma máquina em estado de drenagem em vez de ligar uma máquina.

O Autoscale coloca máquinas em excesso em "estado de drenagem" uma a uma:

- Se duas ou mais máquinas tiverem o mesmo número de sessões ativas, o Autoscale drena a máquina que esteve ligada pelo atraso de desligamento especificado.

  Fazer isso evita colocar máquinas recém-ligadas em estado de drenagem, pois essas máquinas são mais propensas a ter o menor número de sessões.
- Se duas ou mais máquinas estiveram ligadas pelo atraso de desligamento especificado, o Autoscale drena essas máquinas uma a uma aleatoriamente.

Máquinas em estado de drenagem não hospedam mais novos inícios de sessão e estão aguardando que as sessões existentes sejam encerradas. Uma máquina se torna candidata a desligamento somente quando todas as sessões são encerradas. No entanto, se não houver

máquinas imediatamente disponíveis para inícios de sessão, o Autoscale prefere direcionar os inícios de sessão para uma máquina em estado de drenagem em vez de ligar uma máquina.

Uma máquina é retirada do estado de drenagem quando uma das seguintes condições é atendida:

- A máquina é desligada.
- O Autoscale está desabilitado para o grupo de entrega ao qual a máquina pertence.
- O Autoscale usa a máquina para atender aos requisitos de agendamento ou demanda de carga. Este caso ocorre quando o agendamento (escalonamento baseado em agendamento) ou a demanda atual (escalonamento baseado em carga) exige mais máquinas do que o número de máquinas atualmente ligadas.

> **Importante:**

> Se nenhuma máquina estiver imediatamente disponível para inícios de sessão, o Autoscale prefere direcionar os inícios de sessão para uma máquina em estado de drenagem em vez de ligar uma máquina. Uma máquina em estado de drenagem que hospeda um início de sessão permanece em estado de drenagem.

> Para descobrir quais máquinas estão em estado de drenagem, use o comando PowerShell `Get-BrokerMachine`. Por exemplo: `Get-BrokerMachine -DrainingUntilShutdown $true`. Alternativamente, você pode usar o Studio. Consulte Exibir máquinas em estado de drenagem.

EXIBIR MÁQUINAS EM ESTADO DE DRENAGEM

> **Nota:**

> Este recurso se aplica apenas a máquinas de várias sessões.

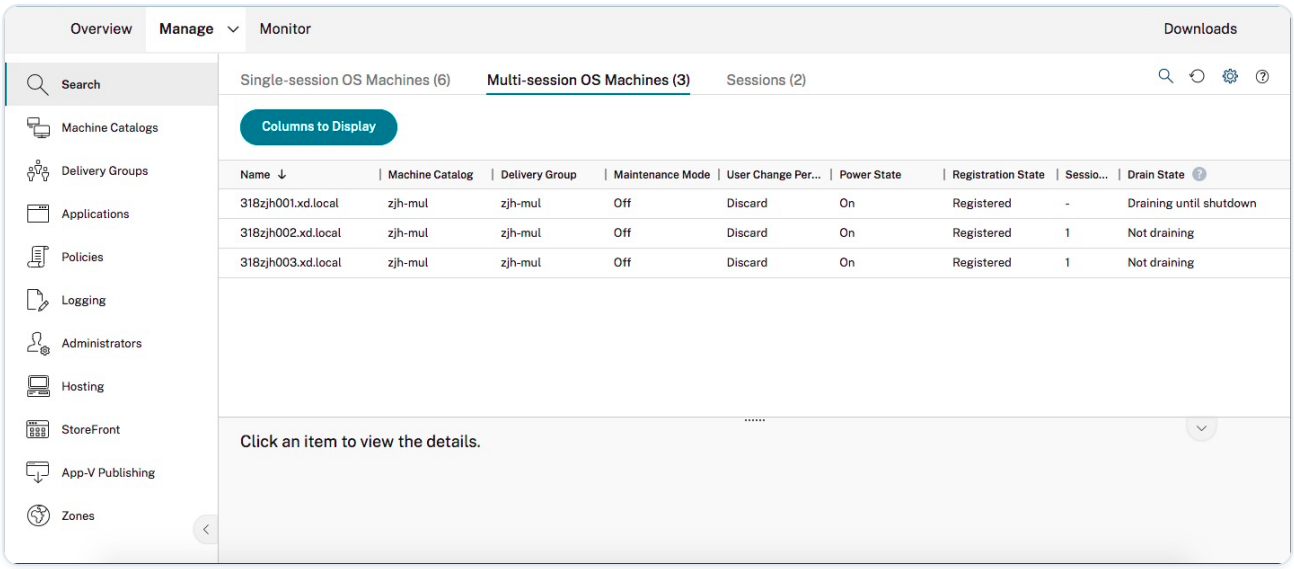
> No Studio, você pode exibir máquinas que estão no estado de drenagem, informando quais máquinas estão prestes a serem desligadas. Conclua as seguintes etapas:

1. navegar para o nó **Pesquisar** e, em seguida, clique em **Colunas a Exibir**.
2. Na janela **Colunas a Exibir**, selecione a caixa de seleção ao lado de **Estado de Drenagem**.

3. Clique em **Salvar** para sair da janela **Colunas a Exibir**.

A coluna **Estado de Drenagem** pode exibir as seguintes informações:

- **Drenando até o desligamento.** Aparece quando as máquinas estão no estado de drenagem até serem desligadas.
- **Não drenando.** Aparece quando as máquinas ainda não estão em estado de drenagem.

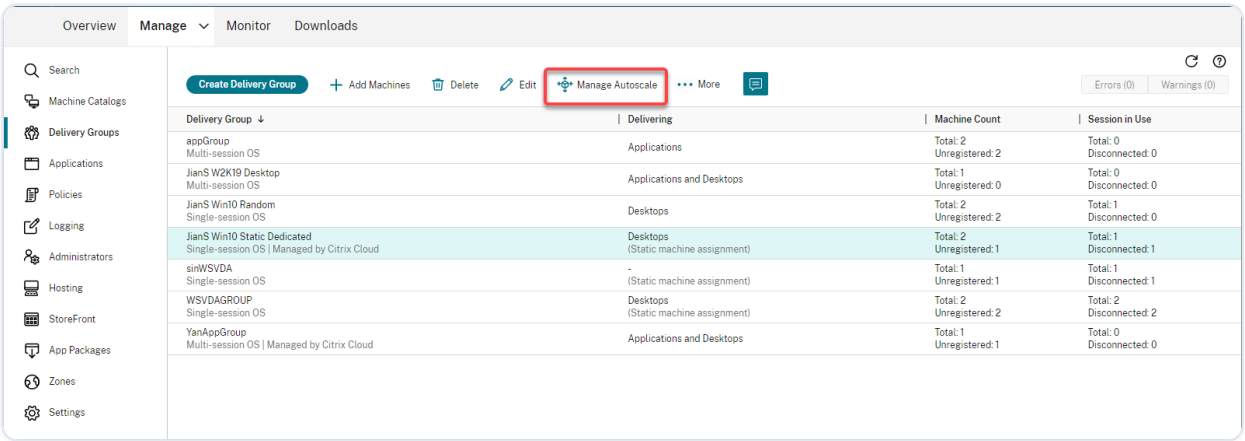


Habilitar o Autoscale para um grupo de entrega

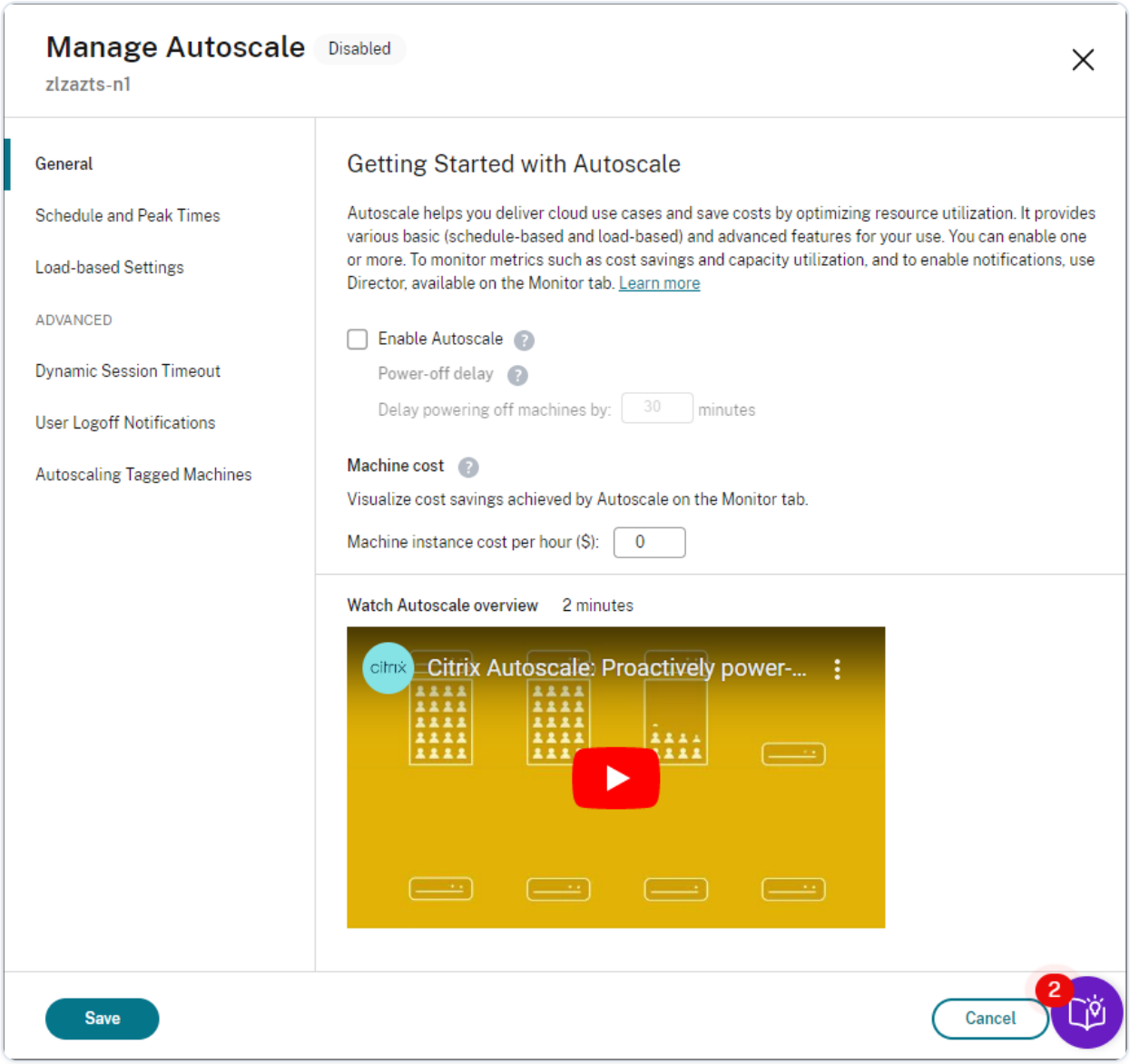
O Autoscale é desabilitado por padrão ao criar um grupo de entrega. Para habilitar e configurar o Autoscale para um grupo de entrega usando o Studio, siga estas etapas:

Você também pode usar comandos do PowerShell para habilitar e configurar o Autoscale para um grupo de entrega. Para obter mais informações, consulte comandos do SDK do PowerShell do Broker.

1. No Studio, selecione **Grupos de Entrega** no painel esquerdo.
2. Selecione o grupo de entrega que você deseja gerenciar e clique em **Gerenciar Autoscale**.



3. Na página **Gerenciar Autoscale**, selecione a caixa de seleção **Habilitar Autoscale** para habilitar o Autoscale. Depois de habilitar o Autoscale, as opções na página são ativadas.



4. Para alterar as configurações padrão com base nas necessidades da sua organização, conclua as seguintes configurações:

   - Configurar agendamentos
   - Para desligar máquinas inativas de forma mais eficiente, use Tempos limite de sessão dinâmicos e Notificações de logoff do usuário
   - Para gerenciar o consumo de energia de um subconjunto de máquinas no grupo de entrega, use Máquinas marcadas com dimensionamento automático

Para desabilitar o Autoscale, desmarque a caixa de seleção **Autoscale**. As opções na página ficam cinzas para indicar que o Autoscale está desabilitado para o grupo de entrega selecionado.

Importante:

- Se você desabilitar o Autoscale, todas as máquinas gerenciadas pelo Autoscale permanecem em seus estados no momento da desabilitação.
- Depois de desabilitar o Autoscale, as máquinas em estado de drenagem são retiradas do estado de drenagem. Para obter mais informações sobre o estado de drenagem, consulte Estado de drenagem.
- As ações de **Políticas de energia** para grupos de entrega estáticos de SO de sessão única e grupos de entrega aleatórios de SO de sessão única na página **Configurações baseadas em carga** são independentes da configuração do Autoscale (habilitado ou desabilitado).

Você pode provisionar máquinas dinamicamente para o grupo usando um script PowerShell. Para obter mais informações, consulte Provisionamento dinâmico de máquinas.

Opções do Autoscale para VMs com sessões de usuário

O Autoscale pode gerenciar máquinas atribuídas e agrupadas, otimizando sua energia e disponibilidade. O conteúdo a seguir fornece comandos PowerShell e configurações de interface do usuário para controlar os estados de energia da máquina com base nos horários de pico e fora de pico e nas sessões de usuário para máquinas atribuídas e agrupadas.

Máquinas atribuídas são dedicadas a um único usuário, enquanto máquinas em pool são compartilhadas entre vários usuários.

Nota:

- As políticas de limite de sessão no Citrix Studio, particularmente o *temporizador de sessão desconectada* e o *temporizador de sessão ociosa*, são cruciais para gerenciar sessões de usuário mesmo quando o Citrix Autoscale NÃO está habilitado. Essas políticas definem por quanto tempo uma sessão pode permanecer desconectada ou ociosa antes de ser encerrada, garantindo a utilização de recursos e evitando sessões bloqueadas. A configuração da política pode ser usada para máquinas atribuídas e em pool, especialmente aquelas que executam VDAs de várias sessões. Para obter informações detalhadas, consulte Configurações da política de limites de sessão.

- O comando PowerShell `Get-BrokerMachine` está obsoleto. Use `Get-BrokerMachineV2` como alternativa.

Para máquinas atribuídas

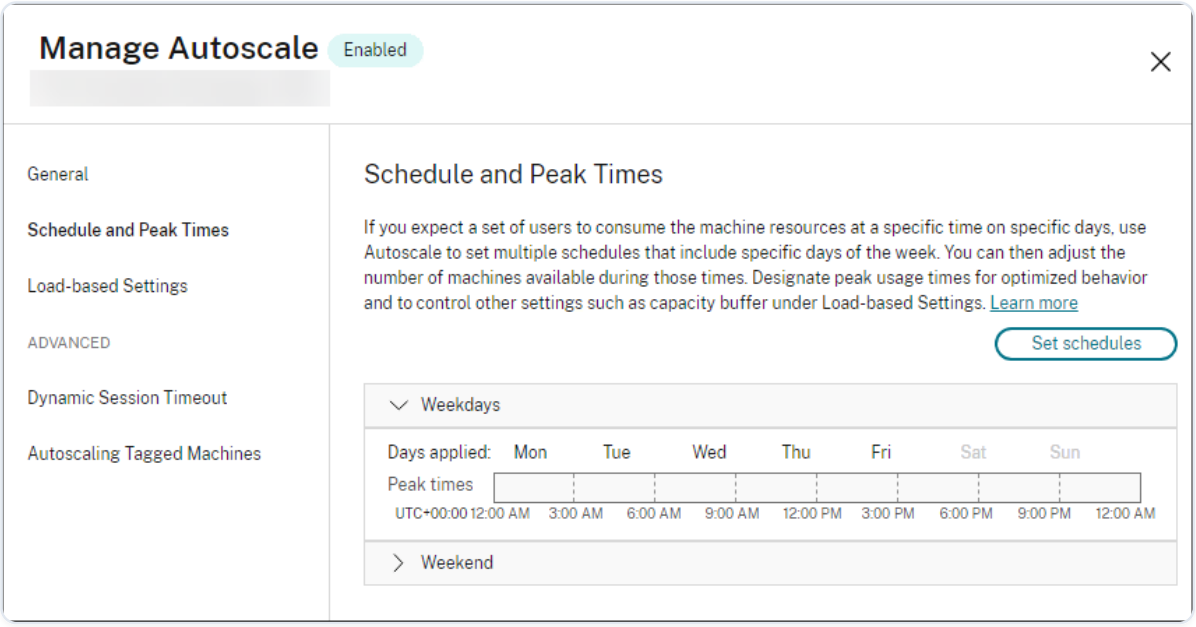
- Para ligar automaticamente máquinas de sessão única atribuídas em um grupo de entrega estático no início do horário de pico, use o comando PowerShell:

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
```

- Para garantir que qualquer máquina atribuída que seja encontrada desligada durante o horário de pico seja reiniciada, habilite também `AutomaticPowerOnForAssignedDuringPeak`.

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
-AutomaticPowerOnForAssignedDuringPeak $True
```

- Se você quiser que as VMs liguem apenas quando um usuário iniciar uma sessão, faça o seguinte:
  - Defina `AutomaticPowerOnForAssigned` e `AutomaticPowerOnForAssignedDuringPeak` como `False`.
  - Defina todas as horas como fora de pico, sem horários de pico, usando a interface do usuário. Consulte Configurações baseadas em agendamento. Durante os horários fora de pico, uma máquina atribuída gerenciada pelo Autoscale é desligada se não houver sessão de usuário nela.



- Nos casos em que todas as máquinas são ligadas pelo Autoscale nos horários de pico, use a interface do usuário para definir o tempo de espera em minutos e ações como, nenhuma ação, suspender ou desligar se nenhum usuário fizer logon após a máquina ser ligada pelo Autoscale. Consulte Políticas de energia.

Para máquinas em pool

Para desligar automaticamente as máquinas em pool após o logoff da sessão, defina o comando PowerShell `ShutdownAfterUse` como `True` para um grupo de entrega. Por exemplo:

```
Set-BrokerDesktopGroup -Name “DesktopGroupName” -ShutdownDesktopsAfterUse $true
```

Monitorar métricas

Depois de habilitar o Autoscale para um grupo de entrega, você pode monitorar as seguintes métricas de máquinas gerenciadas pelo Autoscale no console do **Monitor**.

- Uso da máquina
- Economias estimadas
- Notificações de alerta para máquinas e sessões
- Status da máquina
- Tendências de avaliação de carga

Nota:

> Quando você habilita o Autoscale inicialmente para um grupo de entrega, pode levar alguns minutos para exibir os dados de monitoramento desse grupo de entrega. Os dados de monitoramento permanecem disponíveis se o Autoscale for habilitado e depois desabilitado para o grupo de entrega. O Autoscale coleta dados de monitoramento em intervalos de 5 minutos.

> Para obter mais informações sobre as métricas, consulte Monitorar máquinas gerenciadas pelo Autoscale.

Autoscale em VMs hibernadas

Você pode hibernar VMs por meio de configurações configuráveis do Autoscale. Use os comandos PowerShell `Get-BrokerDesktopGroups`, `New-BrokerDesktopGroups` ou `Set-BrokerDesktopGroups` para definir o seguinte valor positivo para o parâmetro `AutoscaleScaleDownActionDuringPeak` (durante o pico) ou `AutoscaleScaleDownActionDuringOffPeak` (durante o período de inatividade) para definir as ações de energia:

- 0: Desligar as VMs ao reduzir a escala
- 1: Suspender (hibernar as VMs) ao reduzir a escala

VMs que não são capazes de hibernação são desligadas.

Você pode configurar agendamentos de reinicialização para VMs hibernadas se o Grupo de Entrega estiver habilitado para hibernação. No ciclo de reinicialização, as VMs são retomadas e depois desligadas. O agendamento de reinicialização pode ser definido como semanal, diário, mensal e uma vez. Você pode configurar vários agendamentos. No entanto, as VMs que são retomadas da hibernação podem levar alguns minutos.

O Autoscale também pode ligar Serviços de Área de Trabalho Remota (RDS) de várias sessões hibernadas e VMs de sessão única compartilhadas sem sessões ativas durante o horário de pico. As VMs podem ser de catálogos de máquinas MCS e não-MCS.

Mais informações

Para obter mais informações sobre o Autoscale, consulte Citrix Autoscale na Tech Zone.

Configurações baseadas em agendamento e baseadas em carga

Como o Autoscale™ gerencia a energia das máquinas

O Autoscale liga e desliga as máquinas com base no agendamento selecionado. O Autoscale permite que você defina vários agendamentos que incluem dias específicos da semana e ajuste o número de máquinas disponíveis durante esses períodos. Se você espera que um conjunto de usuários consuma os recursos da máquina em um horário específico em dias específicos, o Autoscale ajuda a fornecer uma experiência otimizada. Observe que essas máquinas serão ligadas durante o agendamento, independentemente de haver sessões em execução nelas.

> **Nota:**
>
> O Autoscale oferece suporte a qualquer máquina com gerenciamento de energia.

> O agendamento é baseado no **fuso horário** do grupo de entrega. Para alterar o fuso horário, você pode alterar as configurações do usuário em um grupo de entrega. Para obter mais informações, consulte Gerenciar Grupos de Entrega.

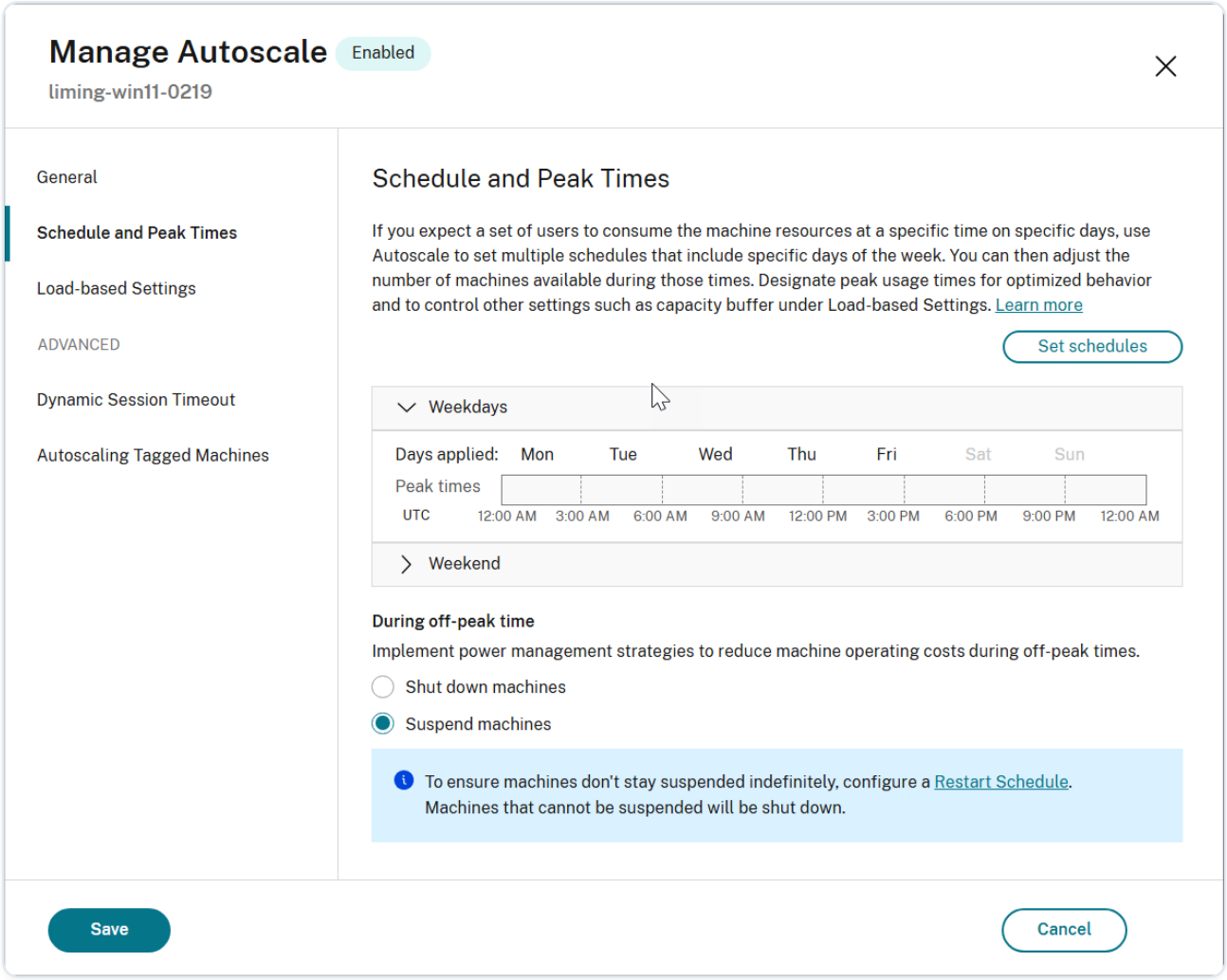
O Autoscale tem dois agendamentos padrão: *Dias da semana* (segunda a sexta-feira) e *Fim de semana* (sábado e domingo). Por padrão, o agendamento de **Dias da semana** mantém uma máquina ligada das 07:00 às 18:30 durante os horários de pico e nenhuma durante os horários de menor movimento. O buffer de capacidade padrão é definido como 10% durante os horários de pico e de menor movimento. Por padrão, o agendamento de **Fim de semana** não mantém nenhuma máquina ligada.

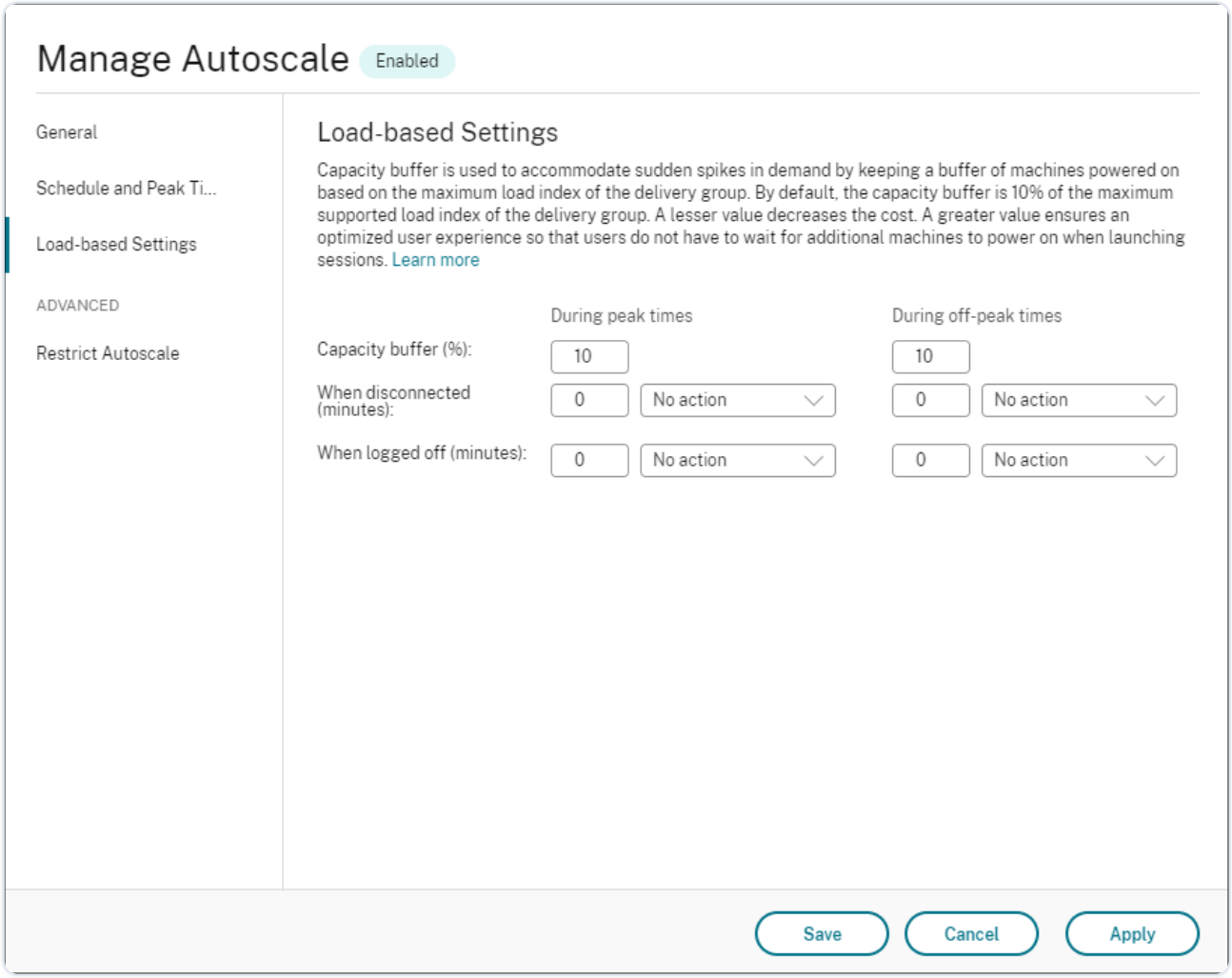
> **Nota:**
>
> O Autoscale considera apenas as máquinas registradas no site como parte da capacidade disponível nos cálculos que ele faz. "Registrada" significa que a máquina está disponível para uso ou já em uso. Isso garante que apenas as máquinas que podem aceitar sessões de usuário sejam incluídas na capacidade do grupo de entrega.

Interfaces de usuário

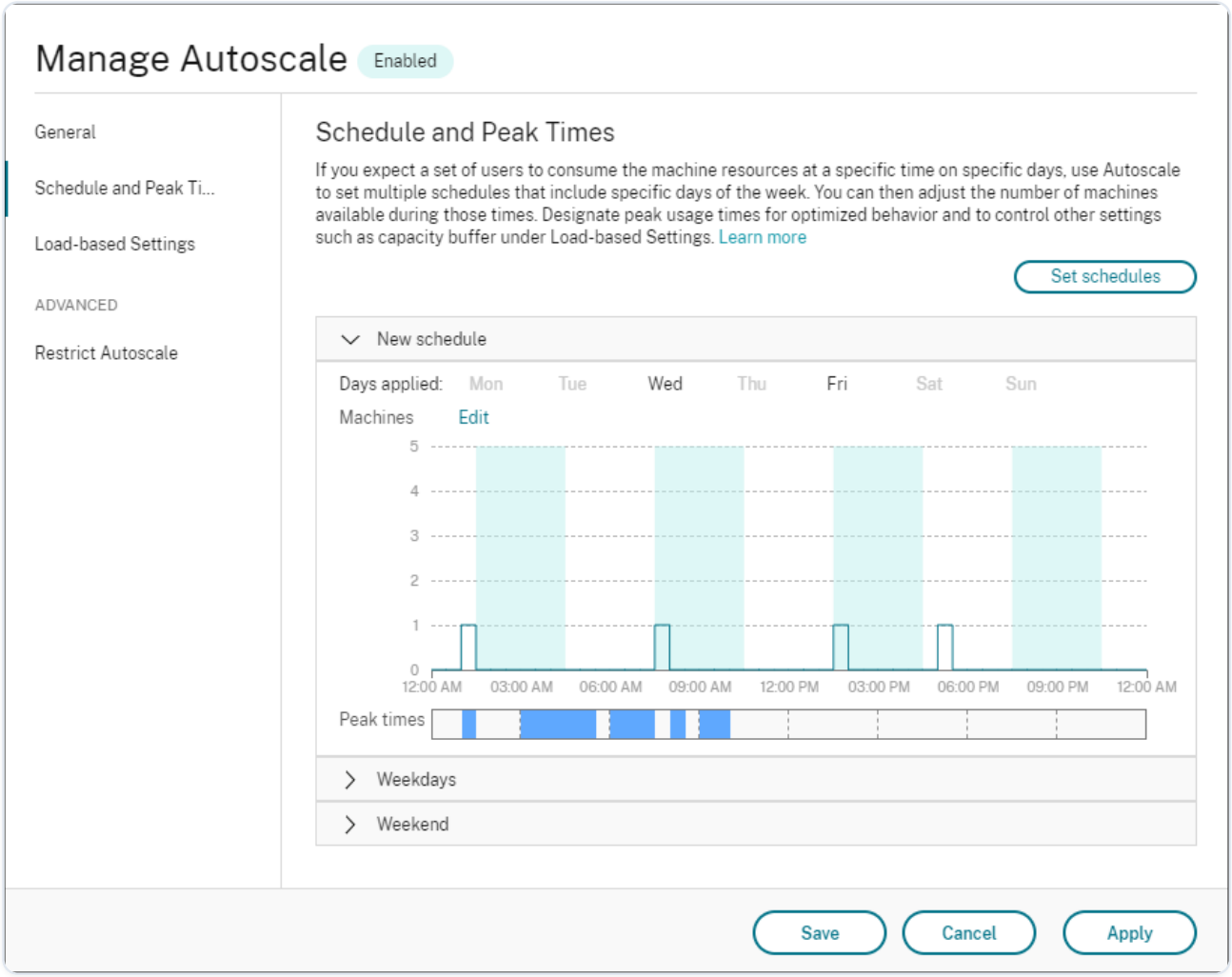
Existem três tipos de interfaces de usuário a serem consideradas.

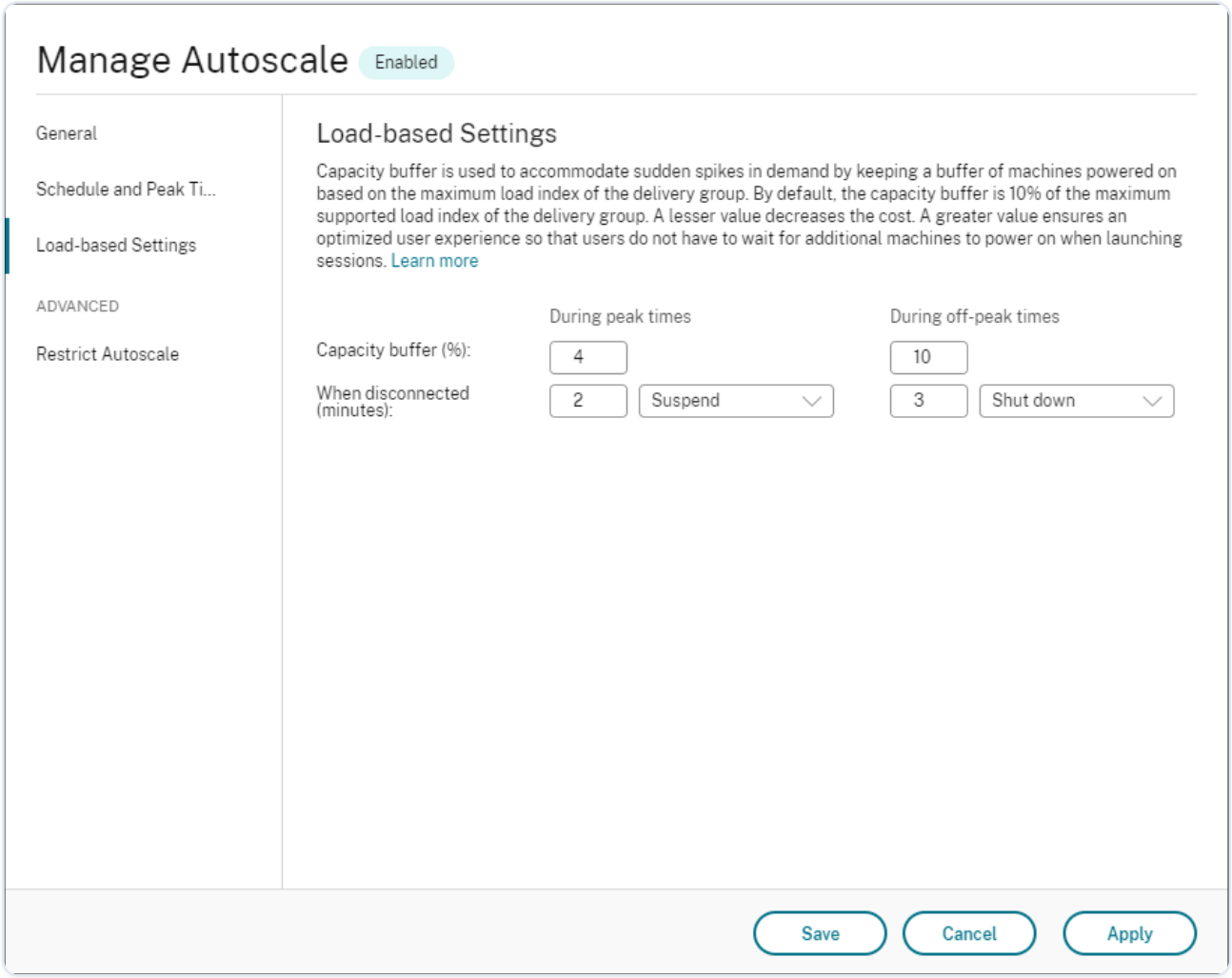
Interface de usuário para *grupos de entrega estáticos de SO de sessão única*:


Manage Autoscale
Enabled
liming-win11-0219
General
Schedule and Peak Times
Load-based Settings
ADVANCED
Dynamic Session Timeout
Autoscaling Tagged Machines
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
Weekdays
Days applied: Mon Tue Wed Thu Fri Sat Sun
Peak times
UTC
12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM
Weekend
During off-peak time
Implement power management strategies to reduce machine operating costs during off-peak times.
Shut down machines
Suspend machines
To ensure machines don't stay suspended indefinitely, configure a Restart Schedule.
Machines that cannot be suspended will be shut down.
Save
Cancel

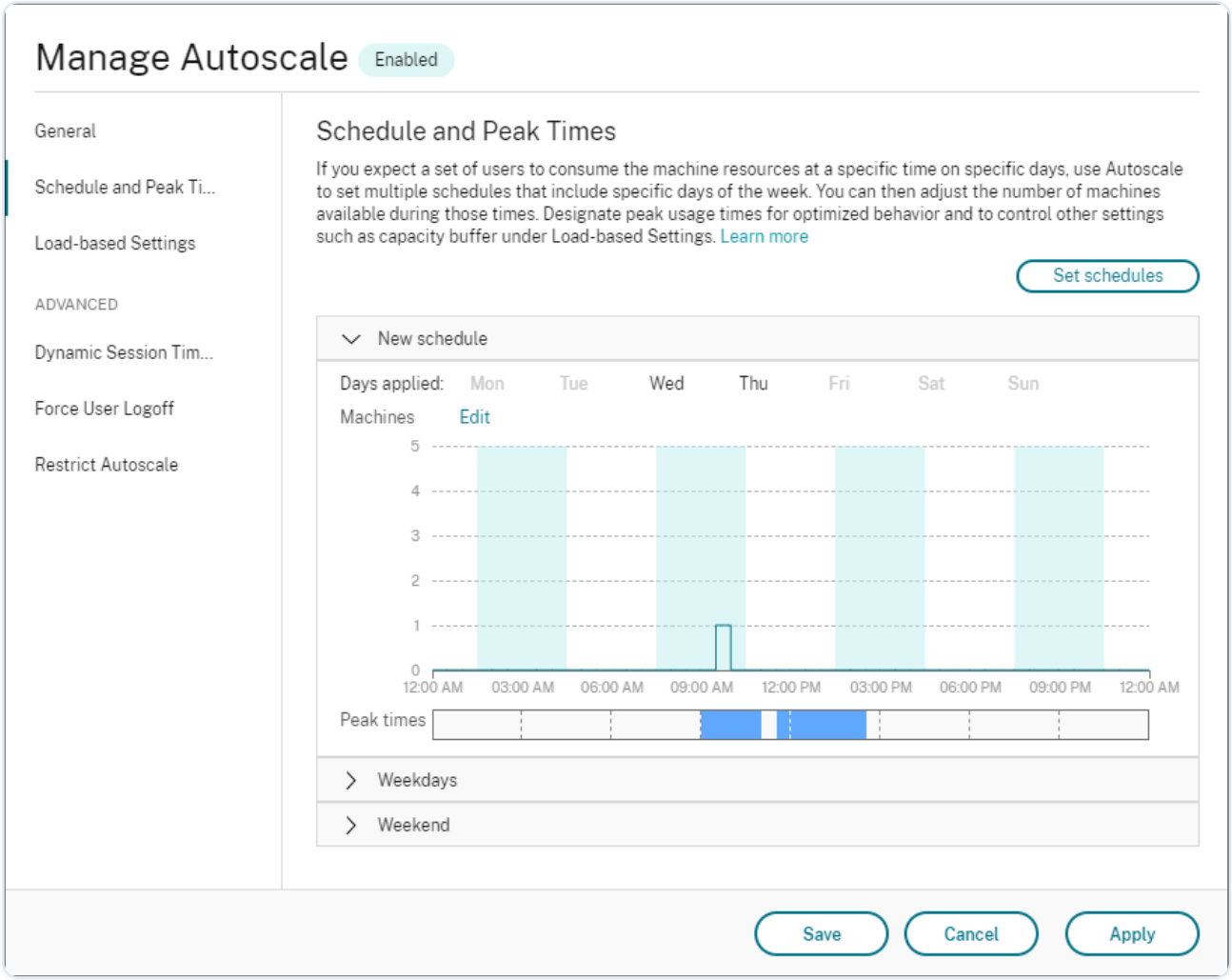


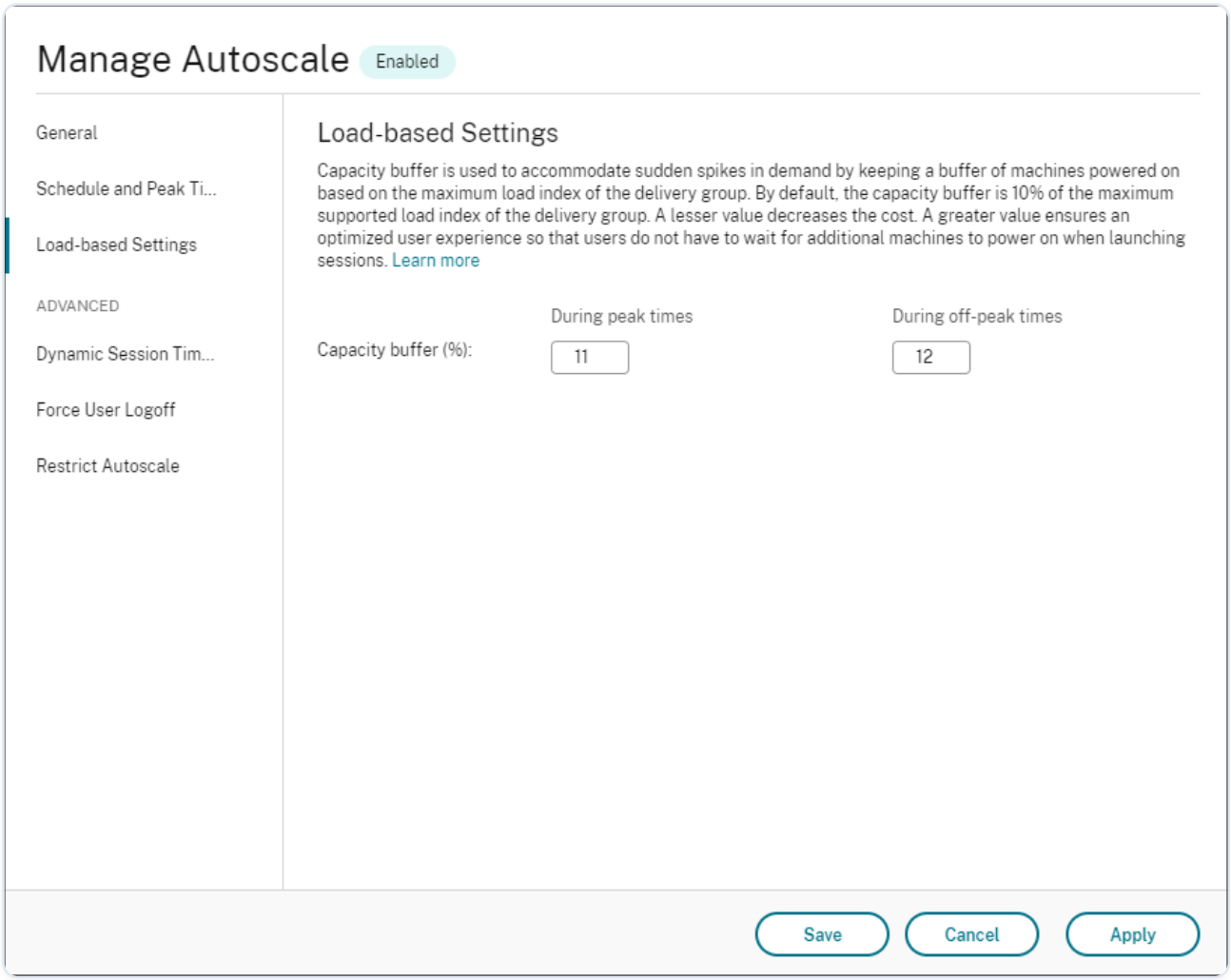
Interface de usuário do Autoscale para *grupos de entrega aleatórios de SO de sessão única*:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM
03:00 AM
06:00 AM
09:00 AM
12:00 PM
03:00 PM
06:00 PM
09:00 PM
12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



Interface de usuário do Autoscale para *grupos de entrega de SO multi-sessão*:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Dynamic Session Tim...
Force User Logoff
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



Configurações baseadas em agendamento

Agendamento do Autoscale. Permite adicionar, editar, selecionar e excluir agendamentos.

Dias aplicados. Destaca os dias que você aplicou ao agendamento selecionado. Os dias restantes ficam esmaecidos.

Editar. Permite atribuir as máquinas a cada hora ou a cada meia hora. Você pode atribuir as máquinas por números e por porcentagens.

Nota:

- Esta opção está disponível apenas nas interfaces de usuário do Autoscale para SO multi-sessão e grupos de entrega aleatórios de SO de sessão única.
- O histograma ao lado de **Editar** plota o número ou a porcentagem de máquinas que estão em execução em diferentes intervalos de tempo.

- Você pode **atribuir máquinas** a cada intervalo de tempo clicando em **Editar** acima de **Horários de pico**. Dependendo da opção selecionada no menu na janela **Máquinas para iniciar**, você pode atribuir as máquinas por números ou por porcentagens.
- Para grupos de entrega de SO multi-sessão, você pode definir o número mínimo de máquinas em execução separadamente em incrementos granulares de 30 minutos durante cada dia. Para grupos de entrega aleatórios de SO de sessão única, você pode definir o número mínimo de máquinas em execução separadamente em incrementos granulares de 60 minutos durante cada dia.

Para definir seus próprios agendamentos, siga estas etapas:

1. Na página **Agendamento e Horários de Pico** da janela **Gerenciar Autoscale**, clique em **Definir agendamentos**.
2. Na janela **Editar Agendamentos do Autoscale**, selecione os dias que deseja aplicar a cada agendamento. Você também pode excluir agendamentos, conforme aplicável.
3. Clique em **Concluído** para salvar os agendamentos e para retornar à página **Agendamento e Horários de Pico**.
4. Selecione o agendamento aplicável e configure-o conforme necessário.
5. Clique em **Aplicar** para sair da janela **Gerenciar Autoscale** ou configurar as definições em outras páginas.

Importante:

- O Autoscale não permite que o mesmo dia se sobreponha em agendamentos diferentes. Por exemplo, se você selecionar segunda-feira no agendamento2 depois de selecionar segunda-feira no agendamento1, a segunda-feira será automaticamente desmarcada no agendamento1.
- Um nome de agendamento não diferencia maiúsculas de minúsculas.
- Um nome de agendamento não deve estar em branco ou conter apenas espaços.
- O Autoscale permite espaços em branco entre os caracteres.
- Um nome de agendamento não deve conter os seguintes caracteres: \ / ; : # . * ? = < > \| ( ) { } " ' `.

- O Autoscale não oferece suporte a nomes de agendamento duplicados. Insira um nome diferente para cada agendamento.
- O Autoscale não oferece suporte a agendamentos vazios. Isso significa que os agendamentos sem dias selecionados não são salvos.

Nota:

Os dias incluídos no agendamento selecionado são destacados, enquanto os não incluídos ficam esmaecidos.

Agendamento de reinício

O Autoscale permite configurar agendamentos de reinício para as máquinas suspensas. Isso garante que os sistemas permaneçam eficientes e evita que os sistemas fiquem suspensos indefinidamente.

Para adicionar um agendamento de reinício para as máquinas suspensas, faça o seguinte:

1. No Studio, selecione **Delivery Groups** no painel esquerdo.
2. Clique com o botão direito do mouse em um grupo de entrega que não tenha um agendamento de reinício e clique em **Gerenciar Autoscale**.
    a. Na página **Geral**, selecione a caixa de seleção **Habilitar Autoscale**.
    b. Na página **Agendamento e Horários de Pico**, selecione a opção **Suspender máquinas** durante os horários de menor movimento. Uma dica para configurar o agendamento de reinício é exibida para evitar que as máquinas fiquem em estado suspenso indefinidamente.
    c. Clique em **Agendamento de Reinício** nas informações da dica.
    d. Configure as configurações preferenciais para **Frequência de reinício**, **Repete a cada**, **Data de início** e **Iniciar reinício em** e clique em **Concluído**.

Configurações baseadas em carga

Horários de pico. Permite definir os horários de pico para os dias aplicados no agendamento selecionado. Você pode fazer isso clicando com o botão direito do mouse no gráfico de barras horizontal. Depois de definir os horários de pico, os horários restantes e não definidos são

padronizados para horários de menor movimento. Por **padrão**, o período das 7:00 AM às 7:00 PM é definido como horários de pico para os dias incluídos no agendamento selecionado.

Importante:

- Para grupos de entrega de SO multi-sessão, o gráfico de barras de horários de pico é usado para o buffer de capacidade.
- Para grupos de entrega de SO de sessão única, o gráfico de barras de horários de pico é usado para o buffer de capacidade e controla as ações a serem acionadas após o logoff e/ou desconexão.
- Você pode definir os horários de pico para os dias incluídos em um agendamento em um nível granular de 30 minutos para grupos de entrega de SO multi-sessão e de SO de sessão única. Alternativamente, você pode usar o comando `New-BrokerPowerTimeScheme PowerShell`. Para mais informações, consulte comandos do SDK do PowerShell do Broker.

Buffer de capacidade. Permite manter um buffer de máquinas ligadas. Um valor menor diminui o custo. Um valor maior garante uma experiência de usuário otimizada para que, ao iniciar sessões, os usuários não precisem esperar que máquinas adicionais sejam ligadas. Por padrão, o buffer de capacidade é de 10% para horários de pico e fora de pico. Se você definir o buffer de capacidade como 0 (zero), os usuários podem ter que esperar que máquinas adicionais sejam ligadas ao iniciar sessões. O Autoscale permite determinar o buffer de capacidade separadamente para horários de pico e fora de pico.

Excluir máquinas em estado de drenagem do buffer de capacidade. Quando selecionado, as máquinas que estão atualmente em drenagem (por exemplo, devido a uma reinicialização agendada) são excluídas do cálculo do buffer de capacidade. Somente máquinas que estão totalmente disponíveis para aceitar novas sessões são contadas ao determinar a capacidade necessária. Isso ajuda a evitar o superprovisionamento que pode ocorrer quando máquinas em drenagem são incluídas no buffer. Por padrão, esta opção não está selecionada. Esta opção está disponível apenas para grupos de entrega de SO de várias sessões e requer o Delivery Controller versão 2503 ou posterior.

Agendamento de reinicialização

O Autoscale permite configurar agendamentos de reinicialização para as máquinas suspensas. Isso garante que os sistemas permaneçam eficientes e evita que os sistemas fiquem suspensos indefinidamente.

Para adicionar um agendamento de reinicialização para as máquinas suspensas, faça o seguinte:

1. Na página **Configurações baseadas em carga**, em **Políticas de energia > Após desconexão**, selecione a ação de suspensão. Uma dica para configurar o agendamento de reinicialização é exibida para evitar que as máquinas fiquem em estado suspenso indefinidamente.
2. Clique em **Agendamento de Reinicialização** nas informações da dica.
3. Configure as configurações preferenciais para **Frequência de reinicialização**, **Repetir a cada**, **Data de início** e **Iniciar reinicialização em** e clique em **Concluído**.

Configurações diversas

Dica:

- Você pode optar por configurar as configurações diversas usando o SDK do Broker PowerShell. Para obter mais informações, consulte Comandos do SDK do Broker PowerShell.
- Para entender os comandos do SDK associados às configurações de quando desconectado e quando o logoff é feito, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`.

Quando desconectado. Permite especificar por quanto tempo uma máquina desconectada e bloqueada permanece ligada após a desconexão da sessão antes de ser suspensa ou desligada. Se um valor de tempo for especificado, a máquina é suspensa ou desligada quando o tempo de desconexão especificado expira, dependendo da ação que você configurou. Por padrão, nenhuma ação é atribuída a máquinas desconectadas. Você pode definir ações separadamente para horários de pico e fora de pico. Para fazer isso, clique na seta para baixo e selecione uma das seguintes opções no menu:

- **Nenhuma ação**. Se selecionado, a máquina após a desconexão da sessão permanece ligada. O Autoscale não age sobre ela.
- **Suspender**. Se selecionado, o Autoscale pausa a máquina sem desligá-la quando o tempo de desconexão especificado expira. A seguinte opção fica disponível depois que você seleciona **Suspender**.
    - **Quando não há reconexão em (minutos)**. Máquinas suspensas permanecem disponíveis para usuários desconectados quando eles se reconectam, mas não estão disponíveis para novos usuários. Para tornar as máquinas disponíveis novamente para manipular todas as cargas de trabalho, desligue-as. Especifique o tempo limite, em minutos, após o qual o Autoscale as desliga.
- **Desligar**. Se selecionado, o Autoscale desliga a máquina quando o tempo de desconexão especificado expira.

> **Nota:**
>
> Esta opção está disponível apenas nas interfaces de usuário do Autoscale para grupos de entrega aleatórios e estáticos de SO de sessão única.

Quando o logoff é feito. Permite especificar por quanto tempo uma máquina permanece ligada após o logoff da sessão antes de ser suspensa ou desligada. Se um valor de tempo for especificado, a máquina é suspensa ou desligada quando o tempo de logoff especificado expira, dependendo das ações que você configurou. Por padrão, nenhuma ação é atribuída a máquinas com logoff. Você pode definir ações separadamente para horários de pico e fora de pico. Para fazer isso, clique na seta para baixo e selecione uma das seguintes opções no menu:

- **Nenhuma ação**. Se selecionado, a máquina após o logoff da sessão permanece ligada. O Autoscale não age sobre ela.
- **Suspender**. Se selecionado, o Autoscale pausa a máquina sem desligá-la quando o tempo de logoff especificado expira.
- **Desligar**. Se selecionado, o Autoscale desliga a máquina quando o tempo de logoff especificado expira.

> **Nota:**

> Esta opção está disponível apenas na interface de usuário do Autoscale para grupos de entrega estáticos de SO de sessão única.

Gerenciar energia de máquinas de SO de sessão única em transição para um período de tempo diferente com sessões desconectadas

> **Importante:**
>
> - Este aprimoramento se aplica apenas a máquinas de SO de sessão única com sessões desconectadas. Não se aplica a máquinas de SO de sessão única com sessões com logoff.
> - Para que este aprimoramento entre em vigor, você precisa habilitar o Autoscale para o grupo de entrega aplicável. Caso contrário, as ações da política de energia de desconexão não são acionadas na transição de período.

> Em versões anteriores, uma máquina de SO de sessão única em transição para um período de tempo em que uma ação (ação de desconexão="**Suspender**" ou "**Desligar**") era necessária permanecia ligada. Esse cenário ocorria se a máquina fosse desconectada durante um período de tempo (horários de pico ou fora de pico) em que nenhuma ação (ação de desconexão="**Nada**") era necessária.

A partir desta versão, o Autoscale suspende ou desliga a máquina quando o tempo de desconexão especificado expira, dependendo da ação de desconexão configurada para o período de tempo de destino.

Por exemplo, você configura as seguintes políticas de energia para um grupo de entrega de SO de sessão única:

- Defina `PeakDisconnectAction` como "Nada"
- Defina `OffPeakDisconnectAction` como "Desligar"
- Defina 'OffPeakDisconnectTimeout' como "10"

> **Observação:**

> Para obter mais informações sobre a política de energia de ação de desconexão, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>` e `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`.

> Em versões anteriores, uma máquina de SO de sessão única com uma sessão desconectada durante os horários de pico permanecia ligada ao fazer a transição do pico para o fora de pico. A partir desta versão, as ações de política `OffPeakDisconnectAction` e `OffPeakDisconnectTimeout` são aplicadas à máquina de SO de sessão única na transição de período. Como resultado, a máquina é desligada 10 minutos após a transição para o fora de pico.

Caso você queira reverter para o comportamento anterior (ou seja, não realizar nenhuma ação em máquinas que fazem a transição de pico para fora de pico ou de fora de pico para pico com sessões desconectadas), faça uma das seguintes opções:

- Defina o valor do registro "LegacyPeakTransitionDisconnectedBehaviour" como 1 (verdadeiro; habilita o comportamento anterior). Por padrão, o valor é 0 (falso; aciona as ações da política de energia de desconexão na transição de período).
  - Caminho: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Nome: LegacyPeakTransitionDisconnectedBehaviour
  - Tipo: REG_DWORD
  - Dados: 0x00000001 (1)
- Configure a configuração usando o comando PowerShell `Set-BrokerServiceConfigurationData`. Por exemplo:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Uma máquina deve atender aos seguintes critérios antes que as ações da política de energia possam ser aplicadas a ela na transição de período:

- Tem uma sessão desconectada.
- Não tem ações de energia pendentes.

- Pertence a um grupo de entrega de SO de sessão única que faz a transição para um período de tempo diferente.
- Tem uma sessão que se desconecta durante um determinado período de tempo (horários de pico ou fora de pico) e faz a transição para um período onde uma ação de energia é atribuída.

Como funciona o buffer de capacidade

O buffer de capacidade é usado para adicionar capacidade sobressalente à demanda atual para contabilizar aumentos dinâmicos de carga. Existem dois cenários a serem considerados:

- Para grupos de entrega de SO de várias sessões, o buffer de capacidade é definido como uma porcentagem da capacidade total do grupo de entrega em termos de índice de carga. Para obter mais informações sobre o índice de carga, consulte Índice de carga.
- Para grupos de entrega de SO de sessão única, o buffer de capacidade é definido como uma porcentagem da capacidade total do grupo de entrega em termos do número de máquinas.

Nota:

- Em cenários onde você restringe o Autoscale a máquinas marcadas, o buffer de capacidade é definido como uma porcentagem da capacidade total das máquinas marcadas no grupo de entrega em termos de índice de carga.
- Para grupos de entrega de SO de várias sessões, quando a opção **Excluir máquinas em estado de drenagem do buffer de capacidade** está ativada, as máquinas em drenagem são excluídas do cálculo da capacidade total. O Autoscale liga máquinas adicionais conforme necessário para manter a porcentagem de buffer configurada, com base apenas em máquinas que estão totalmente disponíveis para aceitar novas sessões.

O Autoscale permite definir o buffer de capacidade separadamente para horários de pico e fora de pico. Um valor menor no campo do buffer de capacidade diminui o custo porque o Autoscale liga menos capacidade sobressalente. Um valor maior garante uma experiência de usuário otimizada para que os usuários não precisem esperar que máquinas adicionais liguem ao iniciar sessões. Por padrão, o buffer de capacidade é de 10%.

Importante:

> O buffer de capacidade resulta no ligamento de máquinas quando a capacidade sobressalente total cai para um nível abaixo de "X" por cento da capacidade total do grupo de entrega. Isso reserva a porcentagem necessária de capacidade sobressalente.

Grupos de entrega de SO multi-sessão

Quando as máquinas são ligadas?

> **Importante:**

> Se um agendamento for selecionado, o Autoscale liga todas as máquinas configuradas para serem ligadas no agendamento. O Autoscale mantém esse número especificado de máquinas ligadas durante o agendamento, independentemente da carga.

> Quando o número de máquinas ligadas no grupo de entrega não consegue mais atender ao buffer necessário para honrar a capacidade do buffer em termos de índice de carga, o Autoscale liga máquinas extras. Por exemplo, digamos que seu grupo de entrega tenha 20 máquinas e 3 máquinas estejam agendadas para serem ligadas como parte do dimensionamento baseado em agendamento com um buffer de capacidade de 20%. Eventualmente, 4 máquinas serão ligadas quando não houver carga. Isso ocorre porque um índice de carga de 4 x 10k é necessário como buffer; portanto, pelo menos 4 máquinas precisam ser ligadas. Esse caso pode ocorrer durante horários de pico, aumento da carga nas máquinas, novos inícios de sessão e quando você adiciona novas máquinas ao grupo de entrega. Observe que o Autoscale liga apenas as máquinas que atendem aos seguintes critérios:

- As máquinas não estão em modo de manutenção.
- O hipervisor no qual as máquinas estão sendo executadas não está em modo de manutenção.
- As máquinas estão atualmente desligadas.
- As máquinas não têm ações de energia pendentes.

EXCLUIR MÁQUINAS EM DRENAGEM DO BUFFER DE CAPACIDADE

Por padrão, as máquinas em drenagem (por exemplo, aquelas reiniciando no agendamento) contam para a capacidade total quando o Autoscale calcula o buffer. Você pode excluí-las para que o buffer seja baseado apenas em máquinas que estão totalmente disponíveis para aceitar novas sessões.

Para excluir máquinas em estado de drenagem do buffer de capacidade:

1. No **Web Studio**, selecione **Delivery Groups** no painel esquerdo.
2. Clique com o botão direito do mouse em um grupo de entrega de SO multi-sessão e selecione **Manage Autoscale**.
3. Na página **Configurações baseadas em carga**, em **Buffer de capacidade**, selecione **Excluir máquinas em estado de drenagem do buffer de capacidade**.
4. Clique em **Salvar**.

> **Nota:**
>
> Esta opção está disponível apenas para grupos de entrega de SO multi-sessão e requer o Delivery Controller versão 2503 ou posterior.

Quando as máquinas são desligadas?

> **Importante:**
>
> - Se um agendamento for selecionado, o Autoscale desliga as máquinas com base no agendamento.
> - O Autoscale não desliga as máquinas configuradas no agendamento para serem ligadas durante o agendamento.

Quando há máquinas mais do que suficientes para suportar o número desejado de máquinas ligadas (incluindo o buffer) para o grupo de entrega, o Autoscale desliga as máquinas extras. Este caso pode ocorrer durante horários de pico, diminuição da carga nas máquinas e logoffs de sessão, e quando você remove máquinas do grupo de entrega. O Autoscale desliga apenas as máquinas que atendem aos seguintes critérios:

- As máquinas e o hipervisor no qual as máquinas estão sendo executadas não estão em modo de manutenção.
- As máquinas estão atualmente ligadas.
- As máquinas estão registradas como disponíveis ou aguardando registro após a inicialização.
- As máquinas não têm sessões ativas.

- As máquinas não têm ações de energia pendentes.
- As máquinas satisfazem o atraso de desligamento especificado. Isso significa que as máquinas foram ligadas por pelo menos "X" minutos, onde "X" é o atraso de desligamento especificado para o grupo de entrega.

Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do grupo de entrega**. O grupo de entrega que você deseja que o Autoscale gerencie o consumo de energia contém 10 máquinas (M1 a M10).
- **Configuração do Autoscale**
  - O buffer de capacidade está definido para 10%.
  - Nenhuma máquina está incluída no agendamento selecionado.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões de usuário aumentam.
3. Mais sessões de usuário são iniciadas.
4. A carga da sessão do usuário diminui devido ao encerramento da sessão.
5. A carga da sessão do usuário diminui ainda mais até que a carga da sessão seja tratada apenas por recursos locais.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Nenhuma carga de usuário (estado inicial)
  - Uma máquina (por exemplo, M1) é ligada. A máquina é ligada devido ao buffer de capacidade configurado. Neste caso, 10 (número de máquinas) x 10.000 (índice de carga) x 10% (buffer de capacidade configurado) é igual a 10.000. Portanto, uma máquina é ligada.
  - O valor do índice de carga da máquina ligada (M1) está em uma carga de linha de base (índice de carga igual a 0).
- O primeiro usuário faz logon
  - A sessão é direcionada para ser hospedada na máquina M1.

  - O índice de carga da máquina ligada M1 aumenta e a máquina M1 não está mais em uma carga de linha de base.
  - O Autoscale começa a ligar uma máquina adicional (M2) para atender à demanda devido ao buffer de capacidade configurado.
  - O valor do índice de carga da máquina M2 está em uma carga de linha de base.

- Usuários aumentam a carga
  - As sessões são balanceadas entre as máquinas M1 e M2. Como resultado, o índice de carga das máquinas ligadas (M1 e M2) aumenta.
  - A capacidade sobressalente total ainda está em um nível acima de 10.000 em termos de índice de carga.
  - O valor do índice de carga da máquina M2 não está mais em uma carga de linha de base.

- Mais sessões de usuário começam
  - As sessões são balanceadas entre as máquinas (M1 e M2). Como resultado, o índice de carga das máquinas ligadas (M1 e M2) aumenta ainda mais.
  - Quando a capacidade sobressalente total cai para um nível abaixo de 10.000 em termos de índice de carga, o Autoscale começa a ligar uma máquina adicional (M3) para atender à demanda devido ao buffer de capacidade configurado.
  - O valor do índice de carga da máquina M3 está em uma carga de linha de base.

- Ainda mais sessões de usuário começam
  - As sessões são balanceadas entre as máquinas (M1 a M3). Como resultado, o índice de carga das máquinas ligadas (M1 a M3) aumenta.
  - A capacidade sobressalente total está em um nível acima de 10.000 em termos de índice de carga.
  - O valor do índice de carga da máquina M3 não está mais em uma carga de linha de base.

- A carga da sessão do usuário diminui devido ao encerramento da sessão
  - Depois que os usuários saem de suas sessões ou as sessões ociosas expiram, a capacidade liberada nas máquinas M1 a M3 é reutilizada para hospedar sessões iniciadas por outros usuários.
  - Quando a capacidade sobressalente total aumenta para um nível acima de 10.000 em termos de índice de carga, o Autoscale coloca uma das máquinas (por exemplo, M3) em estado de drenagem. Como resultado, as sessões iniciadas por outros usuários não são

mais direcionadas para essa máquina, a menos que novas alterações ocorram. Por exemplo, a carga do usuário final aumenta novamente ou outras máquinas se tornam as menos carregadas.

- A carga da sessão do usuário continua a diminuir
  - Depois que todas as sessões na máquina M3 são encerradas e o atraso de desligamento especificado expira, o Autoscale desliga a máquina M3.
  - Depois que mais usuários encerram suas sessões, a capacidade liberada nas máquinas ligadas (M1 e M2) é reutilizada para hospedar sessões iniciadas por outros usuários.
  - Quando a capacidade sobressalente total aumenta para um nível acima de 10.000 em termos de índice de carga, o Autoscale coloca uma das máquinas (por exemplo, M2) em estado de drenagem. Como resultado, as sessões iniciadas por outros usuários não são mais direcionadas para essa máquina.
- A carga da sessão do usuário continua a diminuir até que não haja sessões
  - Depois que todas as sessões na máquina M2 são encerradas e o atraso de desligamento especificado expira, o Autoscale desliga a máquina M2.
  - O valor do índice de carga da máquina ligada (M1) está em uma carga de linha de base. O Autoscale não coloca a máquina M1 em estado de drenagem devido ao buffer de capacidade configurado.

> **Nota:**
>
> Para grupos de entrega de SO multi-sessão, todas as alterações na área de trabalho são perdidas quando os usuários encerram as sessões. No entanto, se configurado, as configurações específicas do usuário são transferidas junto com o perfil do usuário.

Grupos de entrega aleatórios de SO de sessão única

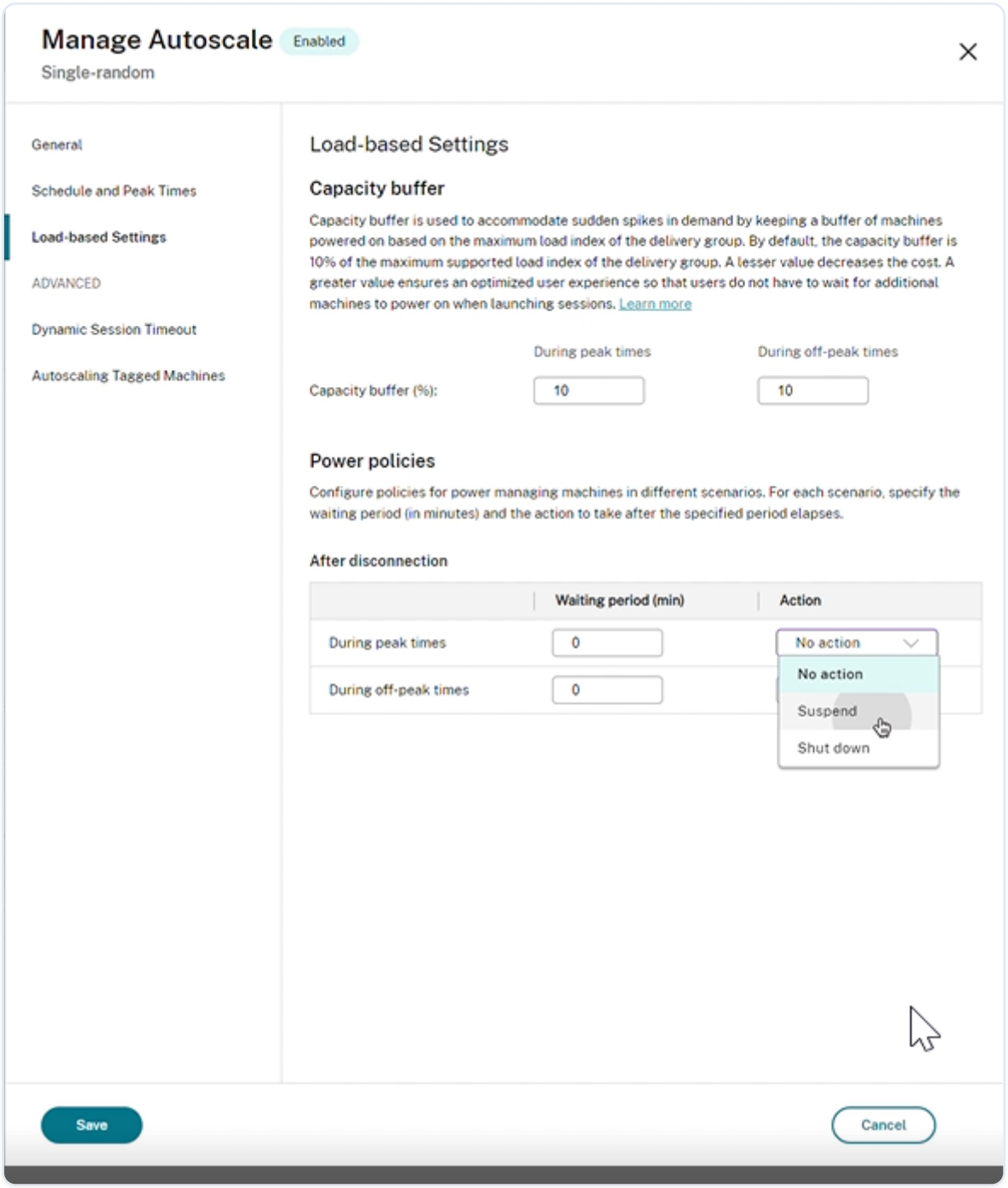
O buffer de capacidade é usado para acomodar picos repentinos de demanda, mantendo um buffer de máquinas ligadas com base no número total de máquinas no grupo de entrega. Por padrão, o buffer de capacidade é 10% do número total de máquinas no grupo de entrega.

Se o número de máquinas (incluindo o buffer de capacidade) exceder o número total de máquinas atualmente ligadas, máquinas adicionais são ligadas para atender à demanda. Se o número de máquinas (incluindo o buffer de capacidade) for menor que o número total de máquinas

atualmente ligadas, as máquinas em excesso são desligadas ou suspensas, dependendo das ações que você configurou.

Políticas de energia

Configure políticas para gerenciar a energia das máquinas para diferentes cenários. Para cada cenário, você pode especificar o tempo de espera (em minutos) e a ação a ser tomada após o término do tempo especificado. As políticas de energia são aplicáveis a grupos de entrega aleatórios de SO de sessão única e grupos de entrega estáticos de SO de sessão única.

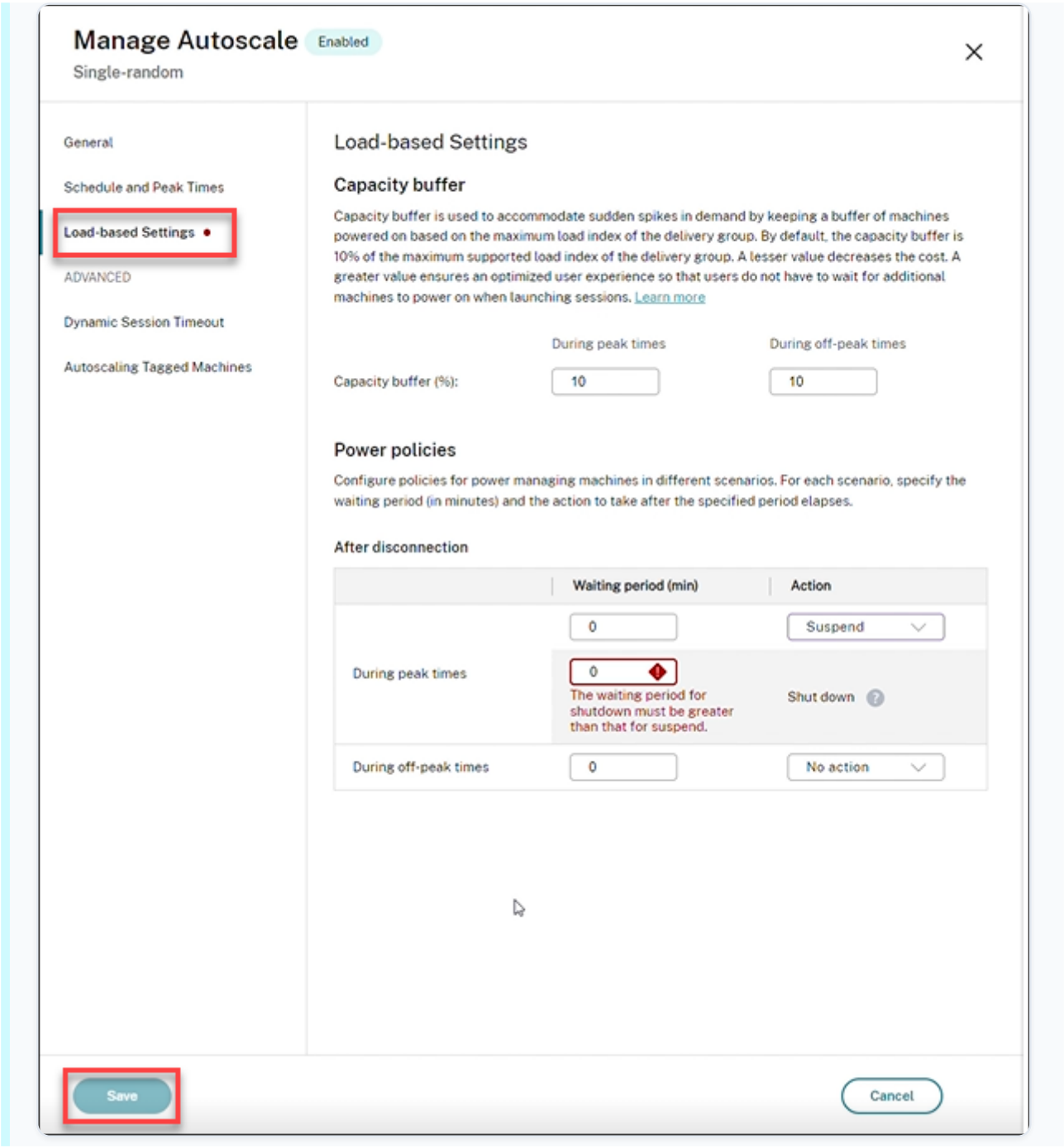


Após a desconexão, as seguintes configurações são aplicáveis tanto durante os horários de pico quanto durante os horários de folga:

- Você pode definir o tempo de espera em minutos e ações como, nenhuma ação, suspender ou desligar no menu suspenso.
- Se você selecionar a ação de suspender, configure um tempo de espera adicional para desligar a máquina.

Nota:

- Durante os horários de pico e de folga, o tempo de espera para a ação de desligamento deve ser maior do que o tempo de espera de suspensão.
- Máquinas suspensas são acessíveis apenas a usuários desconectados quando eles se reconectam. Para tornar as máquinas suspensas disponíveis para novos usuários, desligue-as.
- Se as configurações de tempo estiverem configuradas incorretamente para os campos de suspender e desligar, a opção **Salvar** é desabilitada e um ponto vermelho também aparece ao lado dos itens de navegação, indicando erros de configuração.



Por exemplo

- Se você definir o tempo de espera para 12 minutos e escolher a primeira ação como nenhuma ação, então, após o término de 12 minutos, a máquina continuará no estado ligado.
- Se você definir o tempo de espera para 15 minutos e escolher a primeira ação como suspender e o segundo tempo de espera como 20 minutos, após o término de 15 minutos, a máquina será suspensa. Após o término do segundo tempo de espera, a máquina será desligada.
- Se você definir o tempo de espera para 18 minutos e escolher a primeira ação como desligar, então após o fim dos 18 minutos, a máquina será desligada.

Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do grupo de entrega**. O grupo de entrega que você deseja que o Autoscale gerencie a energia contém 10 máquinas (M1 a M10).
- **Configuração do Autoscale**
  - O buffer de capacidade é definido como 10%.
  - Nenhuma máquina está incluída no agendamento selecionado.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões de usuário aumentam.
3. Mais sessões de usuário são iniciadas.
4. A carga da sessão do usuário diminui devido ao encerramento da sessão.
5. A carga da sessão do usuário diminui ainda mais até que a carga da sessão seja tratada apenas por recursos locais.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Nenhuma carga de usuário (estado inicial)
  - Uma máquina (M1) é ligada. A máquina é ligada devido ao buffer de capacidade configurado. Neste caso, 10 (número de máquinas) x 10% (buffer de capacidade configurado) é igual a 1. Portanto, uma máquina é ligada.
- Um primeiro usuário faz logon
  - Na primeira vez que um usuário faz logon para usar um desktop, o usuário recebe um desktop de um pool de desktops hospedados em máquinas ligadas. Neste caso, o usuário recebe um desktop da máquina M1.
  - O Autoscale começa a ligar uma máquina adicional (M2) para atender à demanda devido ao buffer de capacidade configurado.
- Um segundo usuário faz logon
  - O usuário recebe um desktop da máquina M2.
  - O Autoscale começa a ligar uma máquina adicional (M3) para atender à demanda devido ao buffer de capacidade configurado.

- Um terceiro usuário faz logon
  - O usuário recebe um desktop da máquina M3.
  - O Autoscale começa a ligar uma máquina adicional (M4) para atender à demanda devido ao buffer de capacidade configurado.
- Um usuário faz logoff
  - Depois que um usuário faz logoff ou o desktop do usuário expira, a capacidade liberada (por exemplo, M3) fica disponível como buffer. Como resultado, o Autoscale começa a desligar a máquina M4 porque o buffer de capacidade está configurado para 10%.
- Mais usuários fazem logoff até que não haja mais usuários
  - Depois que mais usuários fazem logoff, o Autoscale desliga as máquinas (por exemplo, M2 ou M3).
  - Mesmo que não haja mais usuários, o Autoscale não desliga a máquina restante (por exemplo, M1) porque essa máquina é reservada como capacidade sobressalente.

> **Nota:**
>
> Para grupos de entrega aleatórios de SO de sessão única, todas as alterações na área de trabalho são perdidas quando os usuários encerram as sessões. No entanto, se configuradas, as configurações específicas do usuário são transferidas junto com o perfil do usuário.

Grupos de entrega estáticos de SO de sessão única

O buffer de capacidade é usado para acomodar picos repentinos de demanda, mantendo um buffer de máquinas não atribuídas ligadas com base no número total de máquinas não atribuídas no grupo de entrega. Por padrão, o buffer de capacidade é 10% do número total de máquinas não atribuídas no grupo de entrega.

> **Importante:**
>
> Depois que todas as máquinas no grupo de entrega são atribuídas, o buffer de capacidade não desempenha um papel na ligação ou desligamento das máquinas.

> Se o número de máquinas (incluindo o buffer de capacidade) exceder o número total de máquinas atualmente ligadas, máquinas adicionais não atribuídas são ligadas para atender à demanda. Se o número de máquinas (incluindo o buffer de capacidade) for menor que o número total de máquinas atualmente ligadas, as máquinas em excesso são desligadas ou suspensas, dependendo das ações que você configurou.

Para grupos de entrega estáticos de SO de sessão única, o Autoscale:

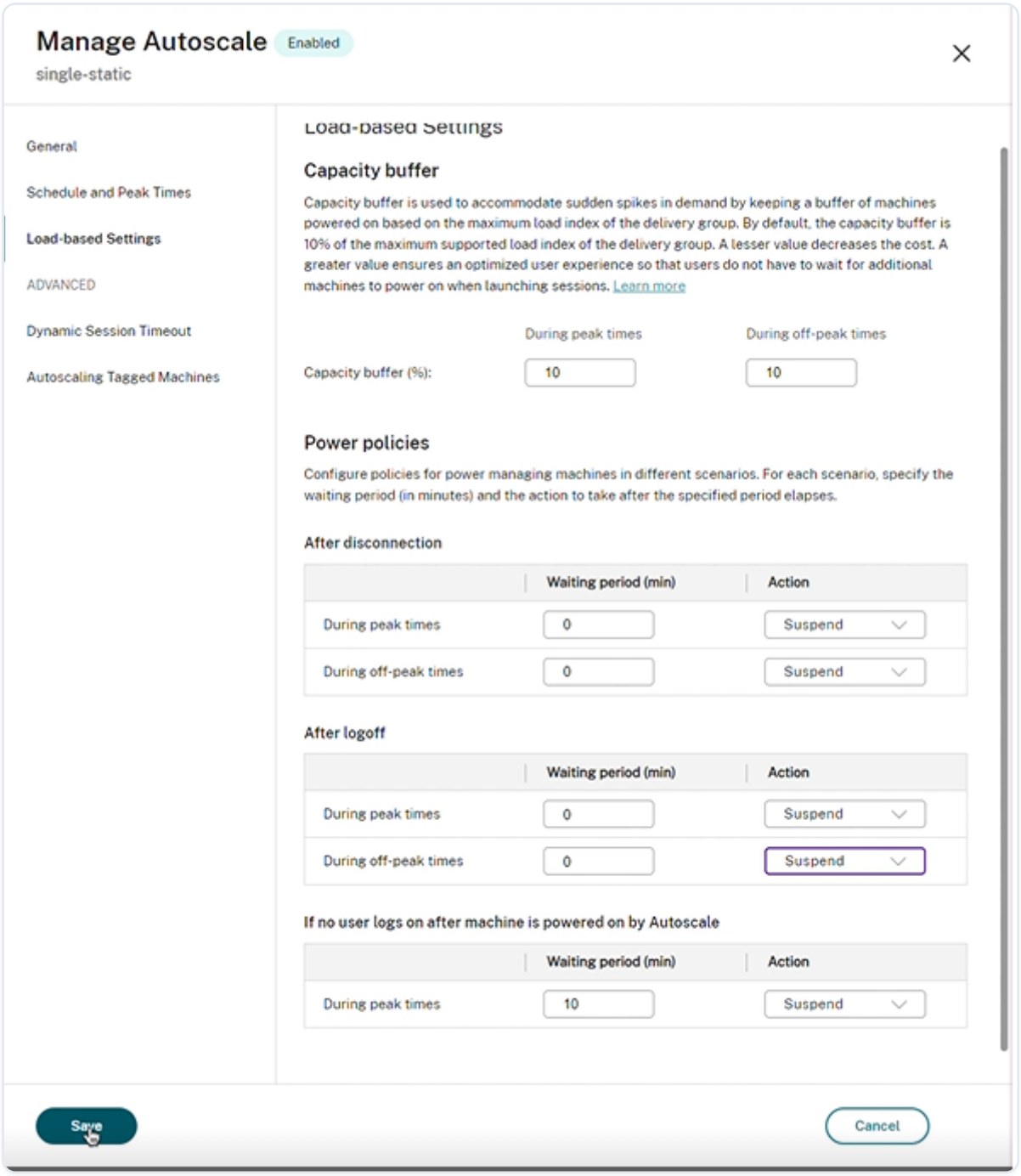
- Liga as máquinas atribuídas durante os horários de pico e as desliga durante os horários de menor movimento somente quando a propriedade `AutomaticPowerOnForAssigned` do grupo de entrega de SO de sessão única aplicável é definida como true.
- Liga automaticamente uma máquina durante os horários de pico se ela estiver desligada e a propriedade `AutomaticPowerOnForAssignedDuringPeak` do grupo de entrega ao qual ela pertence for definida como true.

Para entender como o buffer de capacidade funciona com máquinas atribuídas, considere o seguinte:

- O buffer de capacidade funciona somente quando o grupo de entrega tem uma ou mais máquinas não atribuídas.
- Se o grupo de entrega não tiver máquinas não atribuídas (todas as máquinas no grupo de entrega são atribuídas), o buffer de capacidade não desempenha um papel na ligação ou desligamento das máquinas.
- A propriedade `AutomaticPowerOnForAssignedDuringPeak` determina se as máquinas atribuídas são ligadas durante os horários de pico. Se for definida como true, o Autoscale mantém as máquinas ligadas durante os horários de pico. O Autoscale também as ligará mesmo que estejam desligadas.

Políticas de energia

Configure políticas para gerenciar a energia das máquinas para diferentes cenários. Para cada cenário, você pode especificar o tempo de espera (em minutos) e a ação a ser tomada após o término do tempo especificado. As políticas de energia são aplicáveis a grupos de entrega aleatórios de SO de sessão única e grupos de entrega estáticos de SO de sessão única.



Para **Após desconexão** e **Após logoff**, as seguintes configurações são aplicáveis para ambos, durante horários de pico e durante horários de baixa demanda: Você pode definir o tempo de espera em minutos e ações como, nenhuma ação, suspender ou desligar no menu suspenso.

Se nenhum usuário fizer logon depois que a máquina for ligada pelo Autoscale, as seguintes configurações são aplicáveis apenas durante horários de pico: Você pode definir o tempo de espera em minutos e ações como, nenhuma ação, suspender ou desligar no menu suspenso durante horários de pico.

Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do grupo de entrega**. O grupo de entrega que você deseja que o Autoscale gerencie a energia contém 10 máquinas (M1 a M10).
- **Configuração do Autoscale**
  - As máquinas M1 a M3 são atribuídas, e as máquinas M4 a M10 não são atribuídas.
  - Buffer de capacidade definido para 10% para horários de pico e de baixa demanda.
  - De acordo com o agendamento selecionado, o Autoscale gerencia a energia das máquinas entre 09:00 e 18:00.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Início do agendamento – 09:00
  - O Autoscale liga as máquinas M1 a M3.
  - O Autoscale liga uma máquina adicional (por exemplo, M4) devido ao buffer de capacidade configurado. A máquina M4 não é atribuída.
- Um primeiro usuário faz logon
  - Na primeira vez que um usuário faz logon para usar um desktop, o usuário recebe um desktop de um pool de desktops hospedados em máquinas não atribuídas e ligadas. Neste caso, o usuário recebe um desktop da máquina M4. Logons subsequentes desse usuário se conectam ao mesmo desktop que foi atribuído no primeiro uso.
  - O Autoscale começa a ligar uma máquina adicional (por exemplo, M5) para atender à demanda devido ao buffer de capacidade configurado.
- Um segundo usuário faz logon
  - O usuário recebe um desktop das máquinas não atribuídas e ligadas. Neste caso, o usuário recebe um desktop da máquina M5. Logons subsequentes desse usuário se conectam ao mesmo desktop que foi atribuído no primeiro uso.
  - O Autoscale começa a ligar uma máquina adicional (por exemplo, M6) para atender à demanda devido ao buffer de capacidade configurado.
- Usuários fazem logoff
  - À medida que os usuários fazem logoff de seus desktops ou os desktops expiram, o Autoscale mantém as máquinas M1 a M5 ligadas entre 09:00 e 18:00. Quando esses usuários fazem logon na próxima vez, eles se conectam ao mesmo desktop que foi atribuído no primeiro uso.

    - A máquina não atribuída M6 está aguardando para servir um desktop a um usuário não atribuído que está chegando.

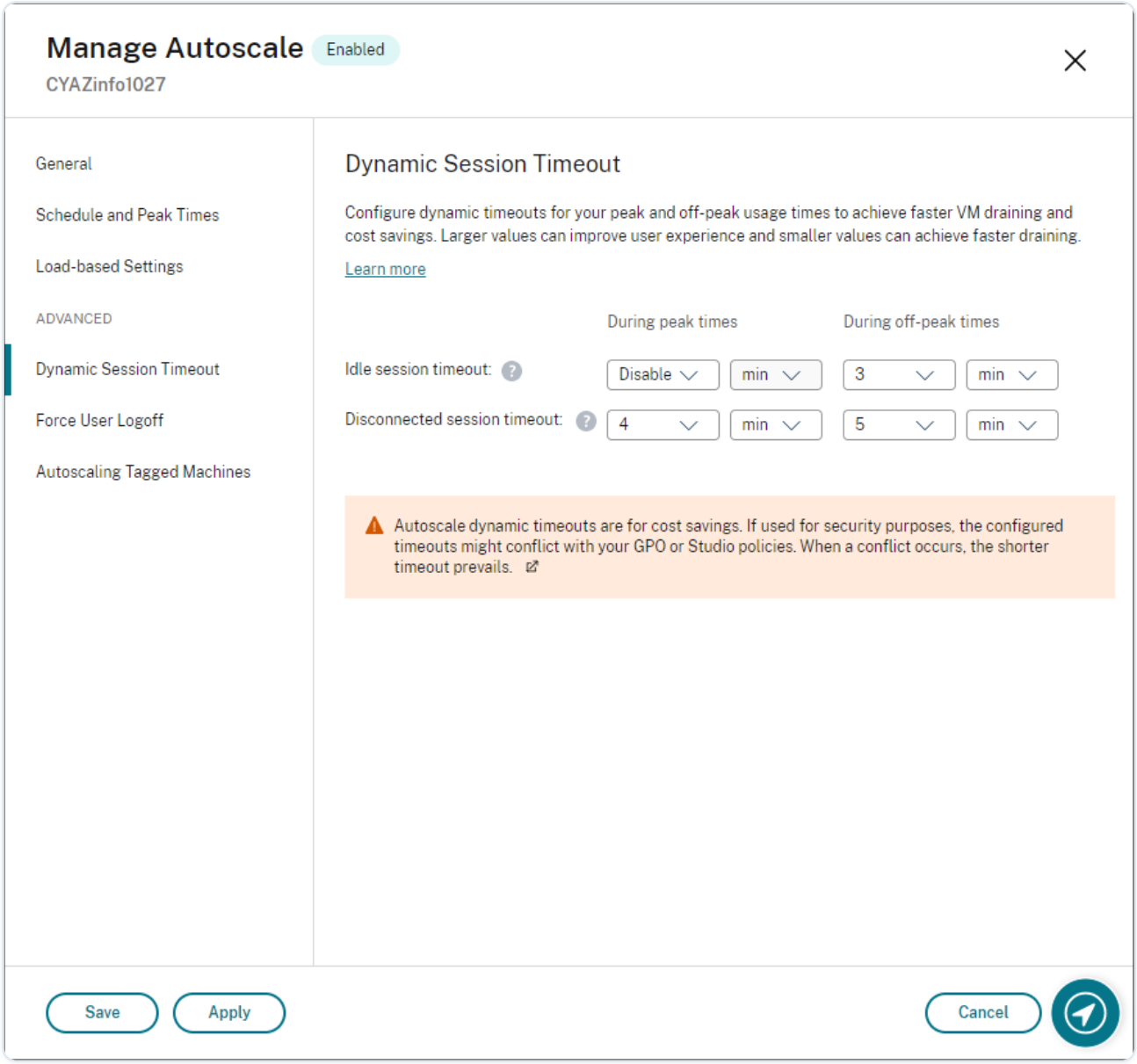
- Fim do agendamento – 18:00
    - Às 18:00, o Autoscale desliga as máquinas M1 a M5.
    - O Autoscale mantém a máquina não atribuída M6 ligada devido ao buffer de capacidade configurado. Essa máquina está aguardando para servir um desktop a um usuário não atribuído que está chegando.
    - No grupo de entrega, as máquinas M6 a M10 são máquinas não atribuídas.

Tempos limite de sessão dinâmicos

Este recurso permite configurar tempos limite de sessão desconectada e ociosa para seus horários de pico e fora de pico de uso, a fim de obter um esvaziamento mais rápido da máquina e economia de custos. Este recurso se aplica a:

- Máquinas de SO de sessão única e de várias sessões.
- Todas as máquinas no Grupo de Entrega, independentemente de estarem marcadas para dimensionamento automático.

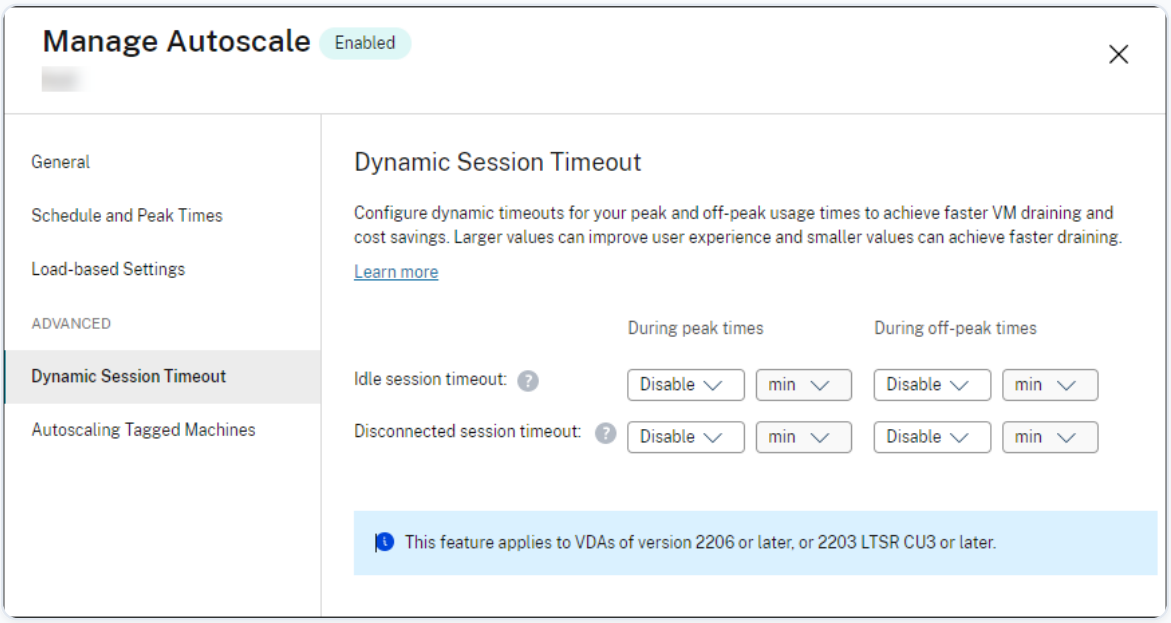
Um VDA relata tempos ociosos para sessões que estiveram ociosas por mais de 10 minutos, portanto, os tempos limite de sessão dinâmicos não conseguirão desconectar sessões ociosas dentro de 10 minutos de inatividade. Um valor menor remove sessões persistentes mais cedo, reduzindo assim os custos.



Nota:

- Este recurso está sempre disponível para grupos de entrega de SO de várias sessões.
- Para grupos de entrega de SO de sessão única, este recurso se aplica a VDAs da versão 2206 CR ou posterior, ou 2203 LTSR CU3 ou posterior. Certifique-se de que esses VDAs tenham se registrado no Citrix Cloud™ pelo menos uma vez. Quando

indisponível, a seguinte interface de usuário aparece:



- Os tempos limite dinâmicos do Autoscale™ são para economia de custos. Se usados para fins de segurança, os tempos limite configurados podem entrar em conflito com suas políticas de GPO ou Studio. Quando ocorre um conflito, o tempo limite mais curto prevalece.

Tempo limite de sessão ociosa. Ativa ou desativa um temporizador que especifica por quanto tempo uma conexão de usuário ininterrupta é mantida se não houver entrada do usuário. Quando o temporizador expira, a sessão é colocada no estado desconectado e o **Tempo limite de sessão desconectada** se aplica. Se o **Tempo limite de sessão desconectada** estiver desativado, a sessão não é encerrada.

Importante:

- Se você especificar um valor menor ou igual a 10 minutos (600 segundos), o Autoscale desconecta as sessões relevantes depois que elas ficam ociosas por 10 minutos. Isso ocorre porque o Autoscale depende dos tempos ociosos de sessão que os VDAs relatam. Os VDAs relatam tempos ociosos apenas para sessões que estiveram ociosas por mais de 10 minutos.
- Uma sessão ociosa ainda será colocada em um estado desconectado se o usuário interagir com ela nos últimos 5 minutos antes de atingir o tempo limite de sessão ociosa.

> **Tempo limite de sessão desconectada**. Ativa ou desativa um temporizador que especifica por quanto tempo uma área de trabalho desconectada permanece bloqueada antes que a sessão seja encerrada. Se ativado, a sessão desconectada é encerrada quando o temporizador expira.

FAQ

O recurso de tempo limite de sessão dinâmico se aplica apenas a máquinas marcadas para Autoscaling?

O recurso de tempo limite de sessão dinâmico aplica-se a todas as máquinas no grupo de entrega, independentemente de estarem marcadas para dimensionamento automático.

Quando uma sessão é desconectada devido ao tempo limite de sessão dinâmico, as máquinas não marcadas também são incluídas no destino do Autoscale de máquinas marcadas?

O recurso de tempo limite de sessão dinâmico não está relacionado ao recurso de marcação do Autoscale. Se os tempos limite de sessão dinâmicos resultarem no encerramento de sessões, máquinas não marcadas também poderão ser desligadas durante o processo, desde que as máquinas estejam esvaziando até o desligamento.

Dimensionamento automático de máquinas marcadas (expansão para a nuvem)

> **Nota:**
>
> Este recurso era anteriormente Restrict Autoscale.

Introdução

O Autoscale oferece a flexibilidade de gerenciar o consumo de energia de apenas um subconjunto de máquinas em um grupo de entrega. Para conseguir isso, aplique uma tag a uma ou mais máquinas e, em seguida, configure o Autoscale para gerenciar o consumo de energia apenas das máquinas marcadas.

Este recurso pode ser útil em casos de uso de expansão para a nuvem, onde você deseja usar recursos locais (ou instâncias de nuvem pública reservadas) para manipular cargas de trabalho antes que os recursos baseados em nuvem atendam à demanda adicional (ou seja, cargas de trabalho de expansão). Para permitir que as máquinas locais (ou instâncias reservadas) atendam

às cargas de trabalho primeiro, você deve usar a restrição de tag juntamente com a preferência de zona.

A restrição de tag especifica as máquinas a serem gerenciadas pelo Autoscale. A preferência de zona especifica as máquinas na zona preferencial para manipular solicitações de inicialização do usuário. Para obter mais informações, consulte Tags e Preferência de zona.

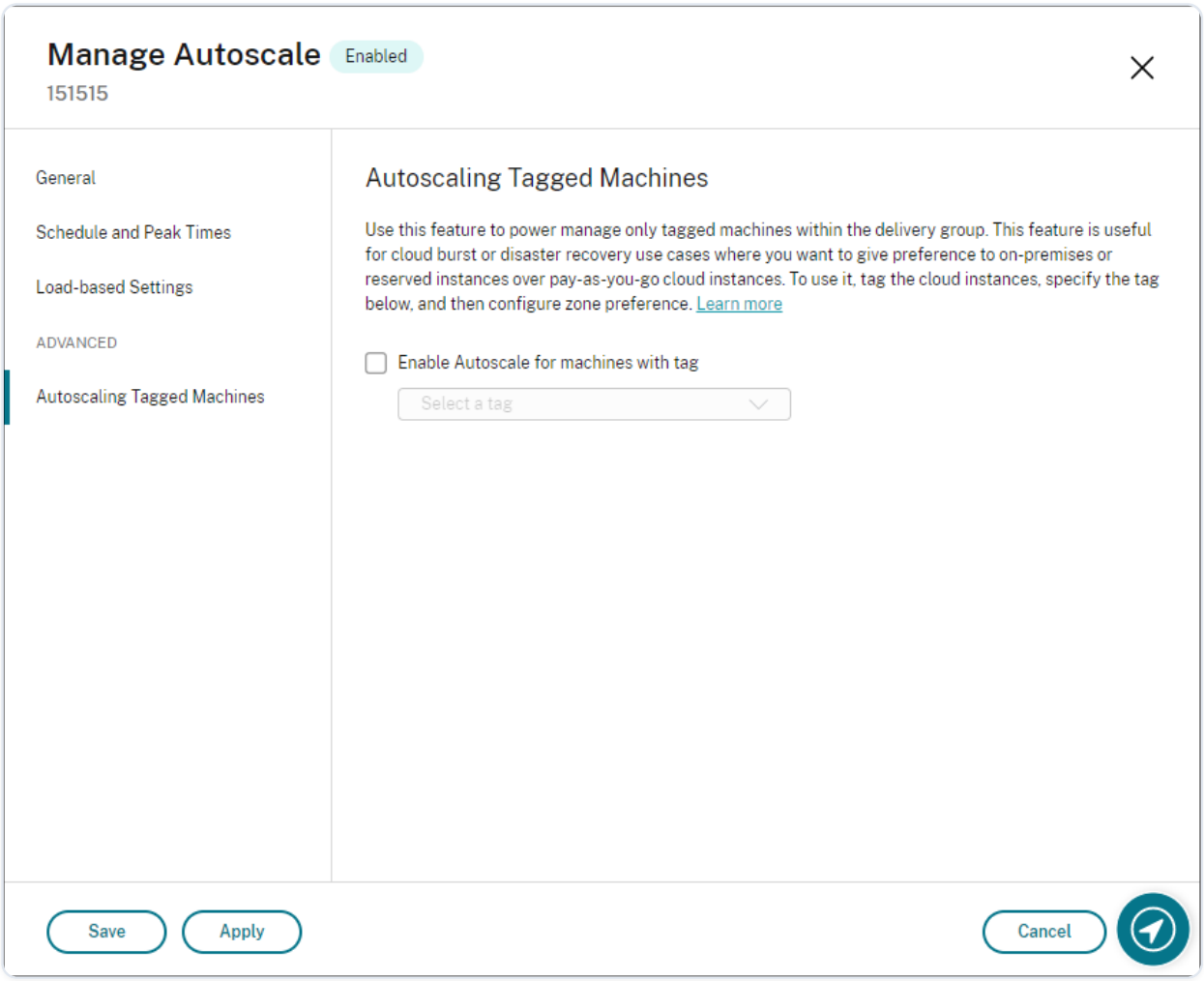
Para dimensionar automaticamente certas máquinas marcadas, você pode usar o Studio ou o PowerShell.

Use o Studio para dimensionar automaticamente certas máquinas marcadas

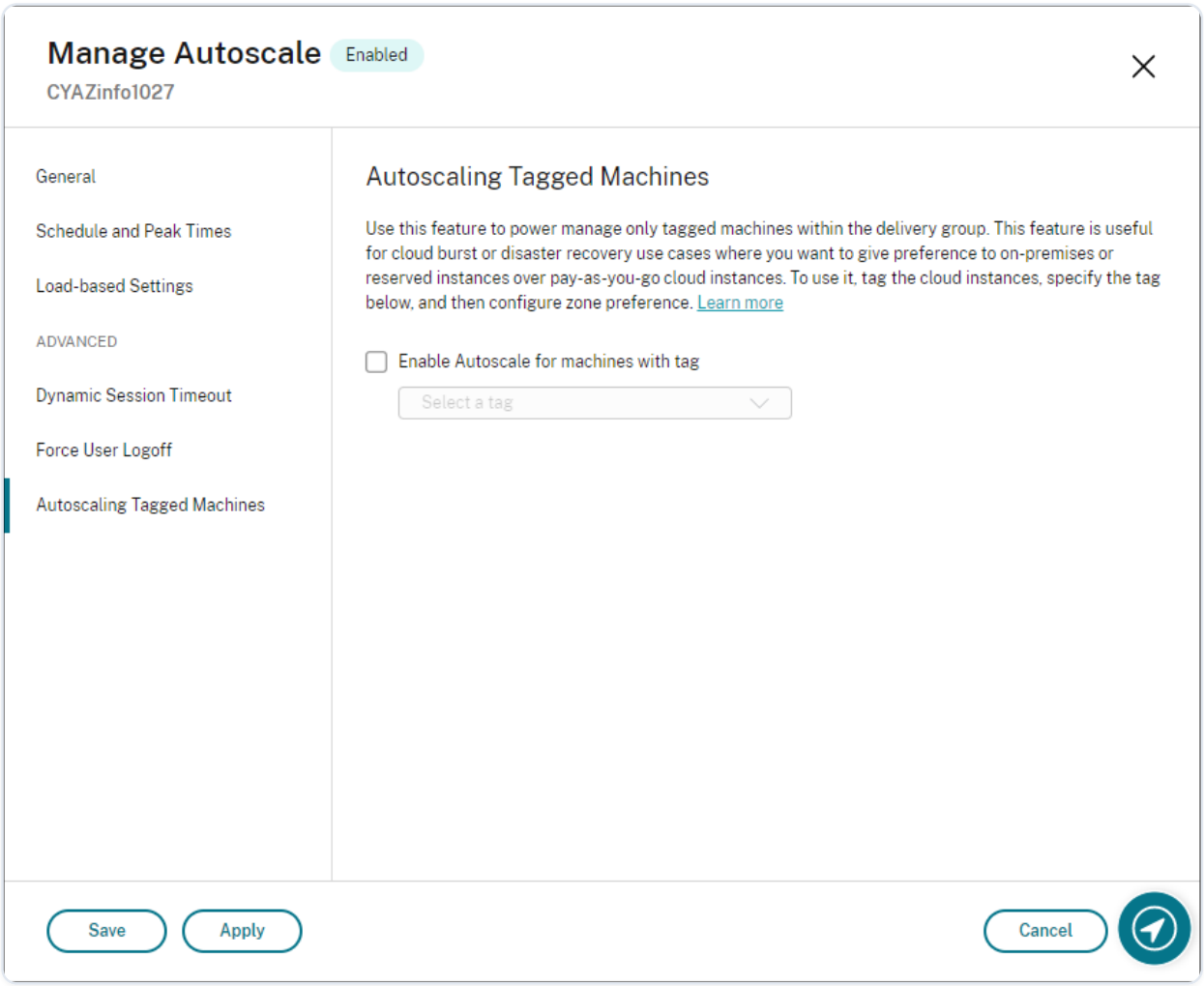
Para dimensionar automaticamente certas máquinas marcadas, conclua as seguintes etapas:

1. Crie uma tag e aplique essa tag às máquinas aplicáveis no grupo de entrega. Para obter mais informações, consulte Gerenciar tags e restrições de tags.
2. Selecione o grupo de entrega e, em seguida, abra o assistente **Gerenciar Autoscale**.
3. Na página **Dimensionamento Automático de Máquinas Marcadas**, selecione **Habilitar Autoscale para máquinas com tag**, selecione uma tag da lista e, em seguida, clique em **Aplicar** para salvar suas alterações.

   Interface do usuário para grupos de entrega *estáticos* e *aleatórios* de SO de sessão única:



Interface de usuário para *grupos de entrega de SO multi-sessão*:



Aviso:

- O dimensionamento automático de máquinas com uma tag específica pode fazer com que o histograma seja atualizado automaticamente para refletir o número de máquinas por tag. Na página **Agendamento e Horários de Pico**, você pode atribuir máquinas manualmente a cada slot de tempo, se necessário.
- Você não pode excluir uma tag que está sendo usada em máquinas marcadas. Para excluir a tag, você deve primeiro remover a restrição da tag.

Depois de aplicar a restrição de tag, você pode querer removê-la do grupo de entrega mais tarde. Para fazer isso, vá para a página **Gerenciar Autoscale > Máquinas Marcadas com Autoscale** e desmarque **Habilitar Autoscale para máquinas com tag**.

Aviso:

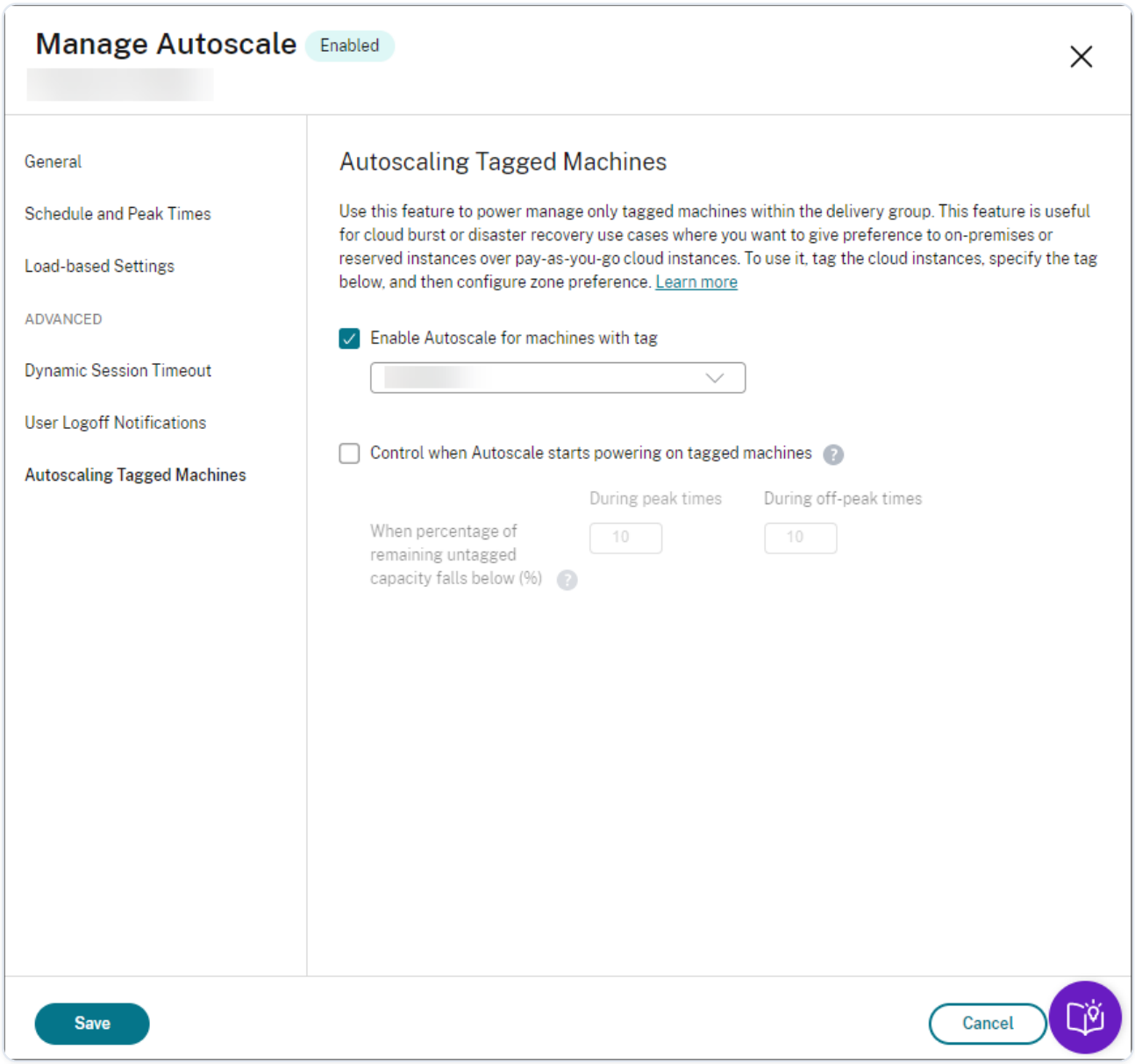
- Se você remover a tag das máquinas aplicáveis sem desmarcar **Habilitar Autoscale para máquinas com tag**, você pode receber um aviso ao abrir o assistente **Gerenciar Autoscale**. Remover a tag das máquinas pode deixar o Autoscale sem máquinas para gerenciar porque a tag especificada no Autoscale se tornou inválida. Para resolver o aviso, vá para a página **Máquinas Marcadas com Autoscale**, remova a tag inválida e clique em **Aplicar** para salvar suas alterações.

Controlar quando o Autoscale liga os recursos

Você também pode controlar quando o Autoscale começa a ligar máquinas marcadas com base no uso de máquinas não marcadas. Isso ajuda você a otimizar ainda mais o consumo de suas cargas de trabalho marcadas ou de nuvem pública.

Para fazer isso, conclua as seguintes etapas:

1. Na página **Máquinas Marcadas com Autoscale**, selecione **Controlar quando o Autoscale começa a ligar máquinas marcadas**.
2. Insira a porcentagem de uso de máquinas não marcadas que você deseja atingir para horários de pico e fora de pico e clique em **Aplicar**. Valores suportados: 0–100.



Dica:

A porcentagem controla quando o Autoscale começa a ligar as máquinas marcadas. Quando a porcentagem cai abaixo do limite (padrão, 10%), o Autoscale começa a ligar as máquinas marcadas. Quando a porcentagem excede o limite, o Autoscale entra no modo de desligamento. Ao inserir a porcentagem, considere dois cenários:

- Para grupos de entrega de SO de sessão única: O valor é definido como uma porcentagem do número total de máquinas não marcadas em estado ocioso. Exemplo: Você tem 10 máquinas de SO de sessão única não marcadas. Quando apenas uma é deixada sem sessão, o Autoscale começa a ligar uma máquina marcada.

- Para grupos de entrega de SO de múltiplas sessões: O valor é definido como uma porcentagem da capacidade total (em termos de índice de carga) de máquinas não marcadas disponíveis. Exemplo: Você tem 10 máquinas de SO de múltiplas sessões não marcadas. Quando elas estão 90% carregadas, o Autoscale começa a ligar uma máquina marcada.

Usar o PowerShell para dimensionar automaticamente certas máquinas marcadas

Nota:

O comando PowerShell `Get-BrokerMachine` está obsoleto. Use `Get-BrokerMachineV2` como alternativa.

Para usar o SDK do PowerShell diretamente, conclua as seguintes etapas:

1. **Crie uma tag.** Use o comando PowerShell New-Brokertag para criar uma tag.
   - Por exemplo: `$managed = New-BrokerTag Managed`. Neste caso, a tag é nomeada "Managed". Para obter mais informações sobre o comando PowerShell New-Brokertag, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>`.
2. **Aplique a tag às máquinas**. Use o comando PowerShell `Get-Brokermachine` para aplicar a tag às máquinas em um catálogo que você deseja que o Autoscale gerencie o consumo de energia.
   - Por exemplo: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. Neste caso, o catálogo é nomeado "cloud".
   - Para obter mais informações sobre o comando PowerShell Get-Brokermachine, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>`.

   Nota:

   Você pode adicionar novas máquinas ao catálogo após aplicar a tag. A tag *NÃO* é aplicada automaticamente a essas novas máquinas.

3. **Adicione máquinas marcadas ao grupo de entrega que você deseja que o Autoscale gerencie o consumo de energia.** Use o comando PowerShell Get-BrokerDesktopGroup para adicionar uma restrição de tag ao grupo de entrega que contém as máquinas (em outras palavras, "restringir inicializações a máquinas com a tag X").

   - Por exemplo: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. Neste caso, o UID do Grupo de Entrega é 1.
   - Para obter mais informações sobre o comando PowerShell Get-BrokerDesktopGroup, consulte `<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`.

Depois de aplicar a restrição de tag, você pode querer removê-la do grupo de entrega mais tarde. Para fazer isso, use o comando PowerShell Get-BrokerDesktopGroup.

Exemplo: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`. Neste caso, o UID do grupo de entrega é 1.

Nota:

Máquinas sem tag são reiniciadas automaticamente depois que os usuários as desligam. Esse comportamento garante que elas se tornem disponíveis para manipular cargas de trabalho mais rapidamente. Isso pode ser ativado ou desativado por grupo de desktop usando a propriedade `AutomaticRestartForUntaggedMachines` de `Set-BrokerDesktopGroup`. Para obter mais informações, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`.

Cenário de exemplo

Suponha que você tenha o seguinte cenário:

- **Configuração do catálogo de máquinas**. Existem dois catálogos de máquinas (C1 e C2).
  - O Catálogo C1 contém 5 máquinas (M1 a M5) que são locais nas implantações no local.
  - O Catálogo C2 contém 5 máquinas (M6 a M10) que são remotas nas implantações na nuvem.

- **Restrição de tag**. Uma tag chamada "Cloud" é criada e aplicada às máquinas M6 a M10 no catálogo C2.
- **Configuração de zona**. Duas zonas (Z1 e Z2) são criadas.
  - A Zona Z1, contendo o catálogo C1, corresponde às implantações no local.
  - A Zona Z2, contendo o catálogo C2, corresponde às implantações na nuvem.
- **Configuração do grupo de entrega**
  - O grupo de entrega contém 10 máquinas (M1 a M10), 5 máquinas dos catálogos C1 (M1 a M5) e 5 do catálogo C2 (M6 a M10).
  - As máquinas M1 a M5 são ligadas manualmente e permanecem ligadas durante todo o agendamento.
- **Configuração do Autoscale**
  - O buffer de capacidade é definido como 10%.
  - O Autoscale gerencia apenas máquinas com a tag "Cloud". Neste caso, o Autoscale gerencia as máquinas em nuvem M6 a M10.
- **Configuração de aplicativo ou desktop publicado**. As preferências de zona são configuradas para os desktops publicados (por exemplo), onde a Zona Z1 é preferida em relação à Zona Z2 para uma solicitação de inicialização do usuário.
  - A Zona Z1 é configurada como a zona preferencial (zona inicial) para os desktops publicados.

O cenário é executado na seguinte sequência:

1. Nenhum usuário faz logon.
2. As sessões de usuário aumentam.
3. As sessões de usuário aumentam ainda mais até que todas as máquinas locais disponíveis sejam consumidas.
4. Mais sessões de usuário são iniciadas.
5. A sessão de usuário diminui devido ao encerramento da sessão.
6. A sessão de usuário diminui ainda mais até que a carga da sessão seja tratada apenas por máquinas locais.

Veja abaixo os detalhes sobre como o Autoscale funciona no cenário acima.

- Nenhuma carga de usuário (estado inicial)
  - As máquinas locais M1 a M5 estão todas ligadas.
  - Uma máquina na nuvem (por exemplo, M6) está ligada. A máquina está ligada devido ao buffer de capacidade configurado. Neste caso, 10 (número de máquinas) x 10.000 (índice de carga) x 10% (buffer de capacidade configurado) é igual a 10.000. Portanto, uma máquina está ligada.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M6) está em uma carga de linha de base (índice de carga igual a 0).
- Usuários fazem logon
  - As sessões são direcionadas para serem hospedadas nas máquinas M1 a M5 através da preferência de zona configurada e são balanceadas entre essas máquinas locais.
  - O valor do índice de carga das máquinas ligadas (M1 a M5) aumenta.
  - O valor do índice de carga da máquina ligada M6 está em uma carga de linha de base.
- Usuários aumentam a carga, consumindo todos os recursos locais
  - As sessões são direcionadas para serem hospedadas nas máquinas M1 a M5 através da preferência de zona configurada e são balanceadas entre essas máquinas locais.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
  - O valor do índice de carga da máquina ligada M6 permanece em uma carga de linha de base.
- Mais um usuário faz logon
  - A sessão excede a preferência de zona e é direcionada para ser hospedada na máquina em nuvem M6.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
  - O valor do índice de carga da máquina ligada M6 aumenta e não está mais em uma carga de linha de base. Quando a capacidade sobressalente total cai para um nível abaixo de 10.000 em termos de índice de carga, o Autoscale começa a ligar uma máquina adicional (M7) para atender à demanda devido ao buffer de capacidade configurado. Observe que pode levar algum tempo para ligar a máquina M7. Portanto, pode haver um atraso até que a máquina M7 esteja pronta.
- Mais usuários fazem logon

  - As sessões são direcionadas para serem hospedadas na máquina M6.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
  - O valor do índice de carga da máquina ligada M6 aumenta ainda mais, mas a capacidade sobressalente total está em um nível acima de 10.000 em termos de índice de carga.
  - O valor do índice de carga da máquina ligada M7 permanece em uma carga de linha de base.

- Ainda mais usuários fazem logon
  - Depois que a máquina M7 estiver pronta, as sessões são direcionadas para serem hospedadas nas máquinas M6 e M7 e são balanceadas entre essas máquinas.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) atingiu 10.000.
  - O valor do índice de carga da máquina M7 não está mais em uma carga de linha de base.
  - O valor do índice de carga das máquinas ligadas (M6 e M7) aumenta.
  - A capacidade sobressalente total ainda está em um nível acima de 10.000 em termos de índice de carga.
- A carga da sessão do usuário diminui devido ao encerramento da sessão
  - Depois que os usuários fazem logoff de suas sessões ou as sessões ociosas expiram, a capacidade liberada nas máquinas M1 a M7 é reutilizada para hospedar sessões iniciadas por outros usuários.
  - Quando a capacidade sobressalente total aumenta para um nível acima de 10.000 em termos de índice de carga, o Autoscale coloca uma das máquinas em nuvem (M6 a M7) em estado de drenagem. Como resultado, as sessões iniciadas por outros usuários não são mais direcionadas para essa máquina (por exemplo, M7), a menos que novas alterações ocorram; por exemplo, a carga do usuário aumenta novamente ou outras máquinas em nuvem se tornam as menos carregadas.
- A carga da sessão do usuário diminui ainda mais até que uma ou mais máquinas em nuvem não sejam mais necessárias.
  - Depois que todas as sessões na máquina M7 são encerradas e o atraso de desligamento especificado expira, o Autoscale desliga a máquina M7.
  - O valor do índice de carga de todas as máquinas ligadas (M1 a M5) pode cair para um nível abaixo de 10.000.
  - O valor do índice de carga da máquina ligada (M6) diminui.

- A sessão do usuário diminui ainda mais até que nenhuma máquina em nuvem seja necessária.
    - Embora não haja sessões de usuário na máquina M6, o Autoscale não a desliga porque ela está reservada como capacidade sobressalente.
    - O Autoscale mantém a máquina em nuvem restante M6 ligada devido ao buffer de capacidade configurado. Essa máquina está aguardando para servir um desktop a um usuário que chega.
    - As sessões não são direcionadas para serem hospedadas na máquina M6 enquanto as máquinas locais tiverem capacidade disponível.

Provisionamento dinâmico de máquinas

O Autoscale™ oferece a capacidade de criar e excluir máquinas dinamicamente. Você pode aproveitar essa capacidade usando um script PowerShell. O script ajuda a escalar dinamicamente o número de máquinas no grupo de entrega para cima ou para baixo com base nas condições de carga atuais.

O script oferece os seguintes benefícios (e mais):

- **Redução dos custos de armazenamento**. Diferente do Autoscale, que ajuda a reduzir seus custos de computação, o script oferece uma solução mais econômica para provisionar máquinas.
- **Gerenciamento eficaz das mudanças de carga**. O script ajuda você a manipular as mudanças de carga escalando automaticamente o número de máquinas para cima ou para baixo com base na carga atual do grupo de entrega.

Baixar o script

O script PowerShell está disponível em `<https://github.com/citrix/Powershell-Scripts/tree/master/XAXD/AutoscaleMcs>`.

Como o script funciona

> **Importante:**

> - Você não pode especificar um catálogo de máquinas em mais de um grupo de entrega a ser gerenciado pelo script. Em outras palavras, se vários grupos de entrega

compartilharem o mesmo catálogo de máquinas, o script não funcionará com nenhum desses grupos de entrega.

- Você não pode executar o script simultaneamente para o mesmo grupo de entrega a partir de vários locais.

O script funciona no nível do grupo de entrega. Ele mede a carga (em termos de índice de carga) e então determina se deve criar ou excluir máquinas.

As máquinas criadas por meio deste script são marcadas de forma exclusiva (através do parâmetro `ScriptTag`) para que possam ser identificadas posteriormente. A criação ou exclusão de máquinas é baseada em:

- **Carga percentual máxima de um grupo de entrega**. Especifica o nível máximo no qual as máquinas devem ser criadas para que o Autoscale lide com cargas extras. Quando esse limite é excedido, as máquinas são criadas em lotes para garantir que a carga atual diminua para ou abaixo do limite.
- **Carga percentual mínima de um grupo de entrega**. Especifica o nível mínimo no qual as máquinas criadas por meio deste script que não possuem sessões ativas devem ser excluídas. Quando esse limite é excedido, as máquinas criadas por meio deste script que não possuem sessões ativas são excluídas.

Este script destina-se a monitorar um grupo de entrega e a criar ou excluir máquinas quando o critério de gatilho for atendido. Ele é executado por execução. Isso significa que você precisa executar o script regularmente para que ele funcione conforme o esperado. Recomendamos que você execute o script em um intervalo mínimo de cinco minutos. Isso melhora a capacidade de resposta geral.

O script depende dos seguintes parâmetros para funcionar:

PARÂMETRO	TIPO	VALOR PADRÃO	DESCRIÇÃO
DeliveryGroupName	String	X	Nome do grupo de entrega a ser monitorado para determinar a carga atual. Você pode fornecer uma lista de nomes separados por ponto e vírgula.

PARÂMETRO	TIPO	VALOR PADRÃO	DESCRIÇÃO
			Por exemplo: `Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3' -XdProfileName profile`.
XdProfileName	String	X	Nome do perfil a ser usado para autenticação em servidores remotos. Para obter detalhes sobre a autenticação em servidores remotos usando este parâmetro, consulte API de Autenticação.
HighWatermark	Inteiro	80	Carga percentual máxima (em termos de índice de carga) na qual criar máquinas para o Autoscale lidar com cargas extras.
LowWatermark	Inteiro	15	Carga percentual mínima (em termos de índice de carga) na qual excluir máquinas criadas por meio deste script que não possuem sessões ativas.
MachineCatalogName	String	X	Nome do catálogo de máquinas onde as máquinas devem ser criadas.

PARÂMETRO	TIPO	VALOR PADRÃO	DESCRIÇÃO
MaximumCreatedMachines	Inteiro	-1	Número máximo de máquinas que podem ser criadas em um grupo de entrega especificado. Se o valor for igual ou menor que 0, o script não processa este parâmetro.
ScriptTag	String	AutoscaledScripted	Tag que se aplica a máquinas criadas através do script.
EventLogSource	String	X	Nome da fonte que aparece no Visualizador de Eventos do Windows.

Nota:

Um "X" indica que nenhum valor padrão é especificado para esse parâmetro.

Por padrão, o script requer todos os parâmetros (exceto o parâmetro `ScriptTag`) na primeira vez que é executado. Nas execuções subsequentes, apenas os parâmetros `DeliveryGroupName` e `XdProfileName` são necessários. Opcionalmente, você pode optar por atualizar as cargas percentuais mínima e máxima.

Observe que você deve especificar um único grupo de entrega na primeira vez que executar o script. Por exemplo, o script *não* funciona se você usar o seguinte comando PowerShell para especificar dois grupos de entrega na primeira vez que executar o script:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2' -XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

Em vez disso, primeiro especifique um único grupo de entrega (neste exemplo, dg1) usando o seguinte comando:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1' -XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

Em seguida, use o seguinte comando para executar o script para o segundo grupo de entrega (neste exemplo, dg 2):

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2' -XdProfileName profile`

Pré-requisitos

Para executar o script, certifique-se de que estes pré-requisitos sejam atendidos:

- A máquina reside no mesmo domínio onde as máquinas estão sendo criadas.
- O SDK do PowerShell Remoto está instalado nessa máquina. Para obter mais informações sobre o SDK do PowerShell Remoto, consulte SDKs e APIs.
- Outros pré-requisitos:
  - Um grupo de entrega para monitorar
  - Um catálogo de máquinas criado por meio do Machine Creation Services™ (MCS) que tenha um esquema de provisionamento (modelo) associado
  - Um pool de identidades associado ao esquema de provisionamento
  - Uma fonte de log de eventos a ser criada para que o script possa gravar informações no Log de Eventos do Windows
  - Um cliente seguro que permite autenticar em servidores remotos

Permissões, recomendações e avisos

Ao executar o script, tenha em mente o seguinte:

- Para autenticar em servidores remotos usando o parâmetro `XdProfileName`, você precisa definir um perfil de autenticação usando um cliente seguro de acesso à API, criado no console do Citrix Cloud. Para obter detalhes, consulte Authentication API.
- Você deve ter permissões para criar e excluir contas de máquina no Active Directory.
- Recomendamos que você automatize o script do PowerShell com o Agendador de Tarefas do Windows. Para obter detalhes, consulte Criar uma tarefa automatizada usando o Agendador de Tarefas do Windows.

- Se você quiser que o script grave informações (por exemplo, falhas e ações) no Log de Eventos do Windows, você precisa primeiro especificar um nome de origem usando o cmdlet `New-EventLog`. Por exemplo, `New-EventLog -LogName Application –Source <sourceName>`. Você pode então visualizar os eventos no painel **Aplicativo** do Visualizador de Eventos do Windows.
- Se ocorrerem erros durante a execução do script, execute o script manualmente e, em seguida, solucione os problemas realizando verificações no script.

API de Autenticação

Antes de executar o script, você precisa definir um perfil de autenticação usando um cliente seguro de acesso à API. Você deve criar um cliente seguro usando a mesma conta sob a qual o script será executado.

O cliente seguro deve ter as seguintes permissões:

- Criar e excluir máquinas usando o MCS.
- Editar catálogos de máquinas (para adicionar e remover máquinas).
- Editar grupos de entrega (para adicionar e remover máquinas).

Ao criar um cliente seguro, certifique-se de que sua conta tenha as permissões acima, pois o cliente seguro herda automaticamente as permissões da sua conta atual.

Para criar um cliente seguro, siga estas etapas:

1. Faça login no Citrix Cloud™ e, em seguida, navegar para **Gerenciamento de Identidade e Acesso > Acesso à API**.
2. Digite o nome do seu cliente seguro e, em seguida, clique em **Criar Cliente**.

Para autenticar em servidores remotos, use o comando PowerShell `Set-XDCredentials`. Por exemplo:

- `Set-XDCredentials -APIKey <key_id> -CustomerId <customer_id> -SecretKey <secret_key> -StoreAs <name specified by the XdProfileName parameter>`

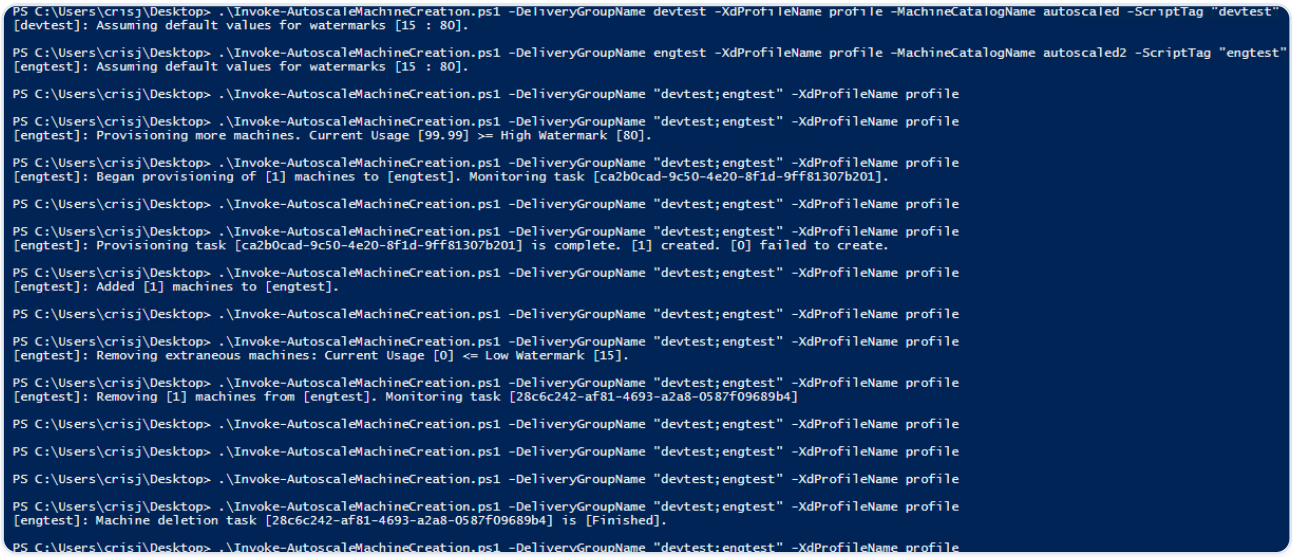
Criar uma tarefa automatizada usando o Agendador de Tarefas do Windows

Você pode automatizar o script PowerShell com o Agendador de Tarefas do Windows. Isso permite que o script seja executado automaticamente em determinados intervalos ou quando certas condições são atendidas. Para executar este script com o Agendador de Tarefas do Windows, certifique-se de selecionar **Não iniciar uma nova instância** na guia **Criar Tarefa >**

Configurações. Isso impede que o Agendador de Tarefas do Windows execute uma nova instância do script se ele já estiver em execução.

Exemplo de execução de script

Veja abaixo um exemplo de execução do script. Observe que o arquivo de script é invocado várias vezes. Neste exemplo, para simular a carga, uma sessão é iniciada e depois encerrada.



Lista de verificação de solução de problemas para o script

O script grava informações (por exemplo, erros e ações) no Log de Eventos do Windows. As informações ajudam você a solucionar problemas que você encontra ao executar o script. Pode ser útil ter em mente a seguinte lista de verificação de solução de problemas:

- Falha na comunicação com servidores remotos. Ações possíveis:
  - Verifique sua conexão com o servidor.
  - Verifique se a chave de API que você usa é válida.
- Falha ao criar máquinas. Ações possíveis:
  - Verifique se a conta de usuário que executa o script tem permissões suficientes para criar contas de usuário no domínio.
  - Verifique se o usuário que criou a chave de API tem permissões suficientes para usar o MCS para provisionar máquinas.
  - Verifique a validade do catálogo de máquinas (ou seja, se sua imagem ainda existe e está em bom estado).

- Falha ao adicionar máquinas a um catálogo de máquinas ou a um grupo de entrega. Ação possível:
    - Verifique se o usuário que criou a chave de API tem permissões suficientes para adicionar e remover máquinas de e para catálogos de máquinas e grupos de entrega.

Plug-in do Autoscale™

O plug-in do Autoscale é um modelo de plug-in onde você pode agir diretamente no gerenciamento de energia de VMs. Você pode desviar das configurações padrão do Autoscale relacionadas ao gerenciamento de energia de VMs e, em vez disso, ter configurações diferentes para cenários diferentes. Atualmente, os plug-ins que você pode usar são:

- Plug-in de feriados do Autoscale
- Plug-in de agendamentos inteligentes do Autoscale

Plug-in de feriados do Autoscale

Você pode usar o plug-in de feriados do Autoscale para manipular configurações diferentes para feriados. Por exemplo, nos dias de semana, você quer que a maioria das VMs esteja ligada. No entanto, por padrão (sem o plug-in), o agendamento de dias de semana ainda é aplicado em feriados públicos. Para manipular este cenário, o plug-in permite que as VMs sejam desligadas em datas de feriado especificadas.

Criar agendamentos de feriados personalizados usando o Studio

Use o Studio para criar agendamentos personalizados para desligar VMs não utilizadas em um grupo de entrega em dias específicos, como feriados, para reduzir o consumo desnecessário de recursos.

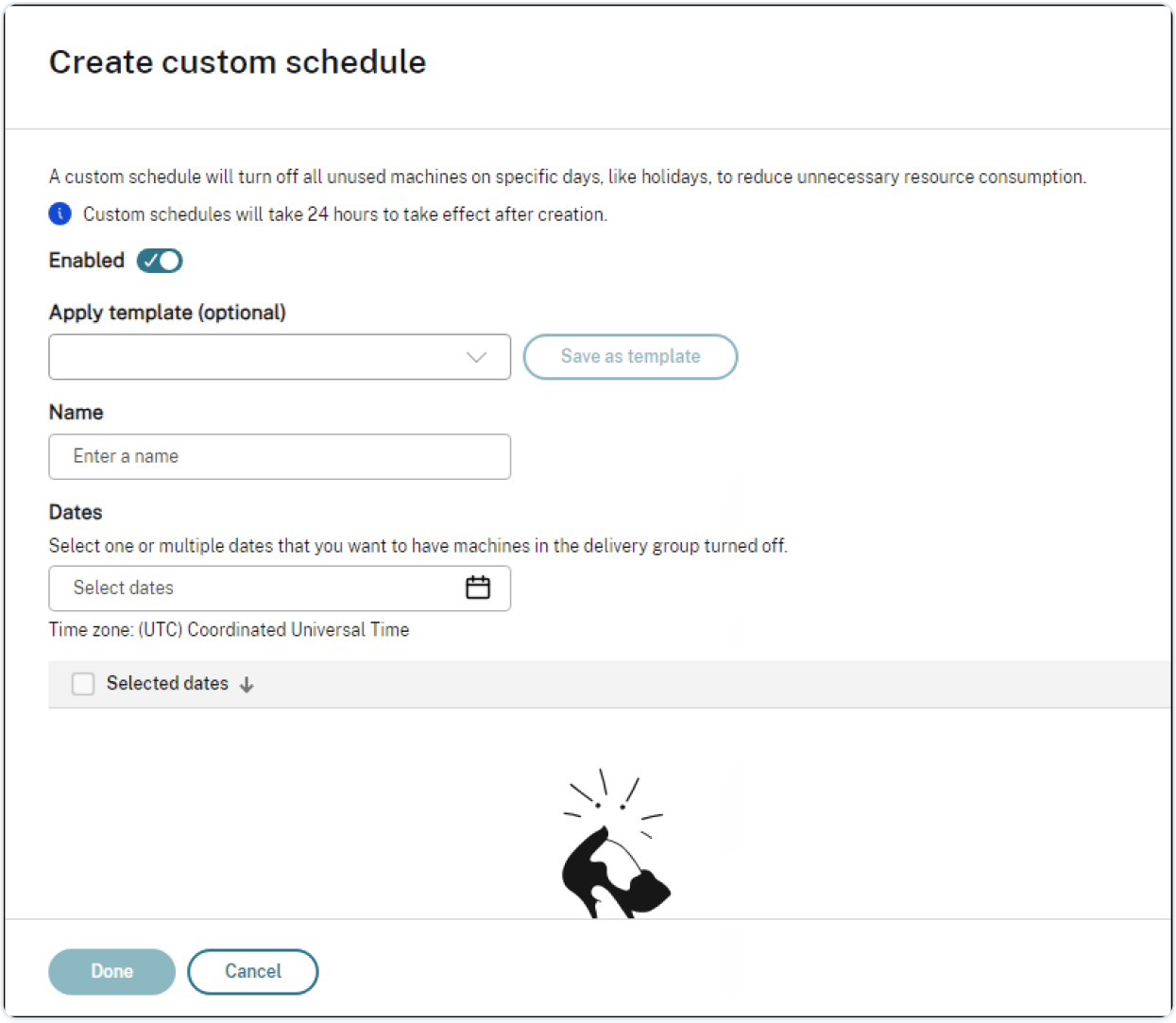
> **Nota:**
>
> O agendamento personalizado entra em vigor um dia após a criação.

Para criar agendamentos personalizados:

1. No Studio, vá para **Grupos de entrega**. Clique com o botão direito em um grupo de entrega e selecione **Gerenciar Autoscale**.
2. Na página **Geral**, selecione **Habilitar Autoscale**.
3. Na página **Agendamento**, clique em **Criar agendamento**.

4. Insira um nome para o agendamento.
5. Selecione uma ou várias datas nas quais você deseja que as VMs no grupo de entrega sejam desligadas.

   Se você quiser salvar este agendamento como um modelo para usar com outros grupos de entrega, clique em **Salvar como modelo**.



6. Clique em **Concluído** para criar o agendamento personalizado.

   Agora você deve ver o agendamento personalizado criado em **Personalizado** na página **Agendamento**.

Para editar um agendamento personalizado:

1. Clique no ícone de lápis em **Ações** para o agendamento que você deseja editar. Você pode fazer as seguintes edições:

   - Desativar o agendamento personalizado: desative o botão de alternância **Ativar**.

- Alterar ou aplicar um modelo.
- Alterar o nome do agendamento.
- Alterar as datas do agendamento.

2. Clique em **Concluído** para aplicar as alterações.

Você também pode excluir um agendamento personalizado.

> **Nota:**
>
> Excluir um grupo de entrega também exclui seus agendamentos personalizados. Os modelos salvos não são excluídos.

Configurar datas de feriado usando PowerShell

Associe o plug-in de feriado do Autoscale a um grupo de entrega e configure as datas de feriado para que o plug-in possa permitir que as VMs sejam desligadas nas datas configuradas. Para conseguir isso, execute os seguintes comandos:

1. Execute `Get-BrokerAutoscalePlugin` para obter o UID do plug-in de feriado.

   ```
   (Get-BrokerAutoscalePlugin -Name
   Citrix.AutoscalePlugin.HolidaySchedule).Uid
   ```

   Anote o valor UID do plug-in `HolidaySchedule`. Vamos supor que o plug-in `HolidaySchedule` tenha UID 1.

2. Obtenha o UID do grupo de entrega ao qual você deseja associar o plug-in. Por exemplo:

   ```
   $dgUid = (Get-BrokerDesktopGroup 'My Group Name').Uid
   ```

3. Associe o plug-in `HolidaySchedule` ao grupo de entrega `(-AutoscalePluginUid “<HolidaySchedule plugin UID>”)` e especifique as datas de feriado necessárias. Por exemplo:

   ```
   New-BrokerAutoscaleGroupPlugin -Name "Company Holidays"
   -DesktopGroupUid $dgUid -AutoscalePluginUid 1 -Configuration
   '{"Holidays":["2024-11-28","2024-11-29","2024-12-25"]}'
   ```

Anote o UID do `AutoscaleGroupPlugin` criado (a associação entre o plug-in e o grupo de entrega).

> **Observação:**
>
> O nome da associação deve ser exclusivo entre as associações para um determinado grupo de entrega. Por exemplo, pode haver apenas uma associação chamada "Feriados da Empresa" para um grupo de entrega, mas um ou mais outros grupos de entrega também podem ter associações chamadas "Feriados da Empresa".

ALTERAR AS DATAS DE FERIADO

Você pode alterar as datas de feriado especificadas usando os comandos PowerShell `Set-BrokerAutoscaleGroupPlugin` e especificando o UID do `AutoscaleGroupPlugin`. Por exemplo, vamos supor que o `AutoscaleGroupPlugin` tenha UID 2.

```
Set-BrokerAutoscaleGroupPlugin 2 -Configuration '{"Holidays":
["2024-11-28","2024-11-29"]}'
```

CONSIDERAÇÕES IMPORTANTES

Considere o seguinte ao trabalhar com o plug-in de feriado do Autoscale:

- Quando o plug-in de feriado do Autoscale está ativo, todos os VDAs são desligados e o sistema não opera com capacidade reduzida. Quaisquer novas solicitações de inicialização são processadas, no entanto, o usuário pode experimentar um atraso devido ao VDA estar sendo preparado para a inicialização.
- O grupo de entrega deve ter um fuso horário especificado.
- O formato da data deve ser "yyyy-mm-dd".
- As substituições de agendamento (que substituem uma configuração padrão do Autoscale) são geradas com um dia de antecedência às 22:00 do dia anterior. Após as 22:00, não é possível adicionar, remover ou alterar nenhuma substituição de agendamento para o dia seguinte.
- O mesmo plug-in do Autoscale pode ser associado a vários grupos de entrega. Execute o `New-BrokerAutoscaleGroupPlugin` para cada grupo de entrega e, em seguida, configure os feriados necessários para esse grupo.

- O comando `Set-BrokerAutoscalePlugin -Configuration` mais recente sobrescreve todos os feriados existentes com os novos feriados especificados.

Plug-in de agendamentos do Autoscale Inteligente

O Autoscale Inteligente é um recurso do Autoscale baseado em dados com configurações administrativas mínimas que permite configurar a meta de desempenho de um grupo de entrega. O valor da meta de desempenho varia de 1 a 99 e o valor especifica um equilíbrio alvo entre a experiência do usuário e o custo:

- Um valor baixo prioriza a economia de custos.
- Um valor alto prioriza a experiência do usuário.

A meta de desempenho, combinada com dados históricos de uso, calcula uma capacidade de buffer ideal (o número de VMs a serem ligadas) para cada bloco de 30 minutos de um dia. Portanto, 48 capacidades de buffer ideais são calculadas no início de cada dia.

A capacidade de buffer ideal substitui a capacidade de buffer de pico/fora de pico e o tamanho do pool para gerenciar as máquinas disponíveis.

Os dados históricos de uso usados para calcular a capacidade de buffer ideal são:

- A taxa de logon do cliente em usuários por minuto
- O tempo médio de inicialização da VM, em minutos
- A densidade média da VM, em usuários por VM.

Pré-requisitos

A seguir estão os requisitos para que o Autoscale Inteligente seja ativado:

- O grupo de entrega deve ser um grupo de entrega compartilhado.
- O grupo de entrega deve ter o Autoscale ativado.
- O grupo de entrega deve ter pelo menos 90 dias de dados históricos antes de configurar o Autoscale inteligente para um grupo de desktop. Você pode aumentar o `ConnectionLogLifetimeHours` de 48 horas para 90 dias usando o comando:

  ```
  Set-BrokerServiceConfigurationData Logging.ConnectionLogLifetimeHours
  -SettingValue 2160.
  ```

Considerações importantes

- O grupo de entrega deve ter um fuso horário especificado.
- As substituições de agendamento são geradas com um dia de antecedência às 22:00 do dia anterior. Após as 22:00, não é possível adicionar, remover ou alterar qualquer substituição de agendamento para o dia seguinte.
- O mesmo plug-in do Autoscale pode ser associado a vários grupos de entrega. Execute o `New-BrokerAutoscaleGroupPlugin` para cada grupo de entrega e, em seguida, configure o destino de desempenho exigido para esse grupo.
- O comando `Set-BrokerAutoscalePlugin -Configuration` mais recente sobrescreve todos os feriados existentes com os novos feriados especificados.

Configurar destino de desempenho

Associe o plug-in `IntelligentAutoscaleSchedules` a um grupo de entrega e configure o destino de desempenho para que o destino de desempenho combinado com os dados de uso históricos possa calcular uma capacidade de buffer ideal para cada bloco de 30 minutos de um dia. Para conseguir isso, execute os seguintes comandos:

1. Execute `Get-BrokerAutoscalePlugi`n para obter o UID do plug-in Autoscale Inteligente. Anote o valor UID do plug-in `IntelligentAutoscaleSchedules`.

   ```
   (Get-BrokerAutoscalePlugin -Name
   Citrix.AutoscalePlugin.IntelligentAutoscaleSchedules).Uid
   ```

   Vamos supor que o plug-in `IntelligentAutoscaleSchedules` tenha UID 2.

2. Obtenha o UID do grupo de entrega ao qual você deseja associar o plug-in. Por exemplo:

   ```
   $dgUid = (Get-BrokerDesktopGroup 'My Group Name').Uid
   ```

3. Associe o plug-in `IntelligentAutoscaleSchedules` ao grupo de entrega (`-AutoscalePluginUid “<IntelligentAutoscaleSchedules value>”`) e especifique o valor do destino de desempenho.

   ```
   New-BrokerAutoscaleGroupPlugin -DesktopGroupUid $dgUid
   -AutoscalePluginUid 2 -Configuration '{"PerformanceTarget":70}'
   ```

4. Observe o UID do `AutoscaleGroupPlugin` criado (a associação entre o plug-in e o grupo de entrega).

Atualizar valor de destino de desempenho

Você pode atualizar o valor de destino de desempenho especificado usando o comando PowerShell `Set-BrokerAutoscaleGroupPlugin` e especificando o UID do `AutoscaleGroupPlugin`. Por exemplo, vamos supor que o AutoscaleGroupPlugin tenha o UID 2.

```
Set-BrokerAutoscaleGroupPlugin 2 -Configuration '{"PerformanceTarget":70}'
```

Configurar aprovação automática do plug-in do Grupo Autoscale

Para permitir a substituição de agendamento (substitui uma configuração padrão do Autoscale), configure as duas propriedades a seguir no `BrokerAutoscaleGroupPlugin`:

- `AutoApprove`
  - Se `True`: Indica que qualquer substituição de agendamento produzida pelo plug-in é automaticamente aceita.
  - Se `False`: O agendamento só é aceito se a data de destino for igual ou anterior à data especificada nas propriedades ApprovedUntil.

  Se `AutoApprove` for `False` e a data `ApprovedUntil` não estiver definida, ou estiver no passado, qualquer substituição de agendamento produzida será descartada sem ser usada.
- `ApprovedUntil`:
  - Se `AutoApprove` for `False`, e você especificar a data `ApprovedUntil`, a substituição de agendamento produzida pelo plug-in será automaticamente aceita como o agendamento para a data de destino.

Por exemplo, vamos supor que o `AutoscaleGroupPlugin` tenha o UID 2.

- Para habilitar a aprovação automática para esse grupo de desktops:

  ```
  Set-BrokerAutoscaleGroupPlugin 2 -AutoApprove $true
  ```

- Para habilitar a aprovação automática até uma data futura:

```
Set-BrokerAutoscaleGroupPlugin 2 -ApprovedUntil "2025-01-01"
```

Notificações de logoff do usuário

Importante:

Este recurso está disponível apenas na interface do usuário do Autoscale™ para grupos de entrega baseados em aplicativos de várias sessões.

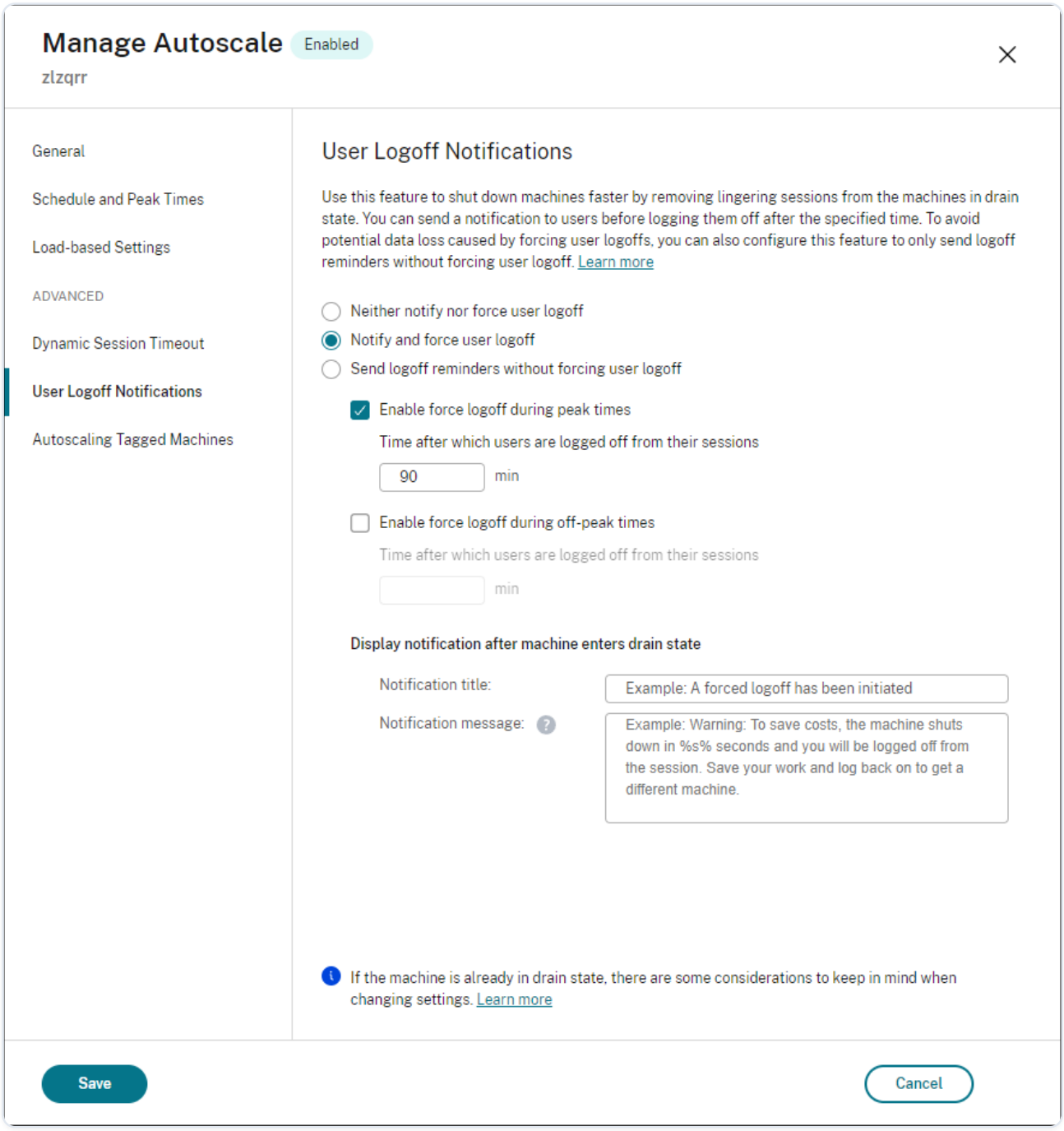
Para melhor alcançar a economia de custos, o Autoscale permite que você force o logoff de sessões persistentes. Ele faz isso permitindo que você envie uma notificação personalizada aos usuários e especifique um período de carência após o qual as sessões são forçadas a fazer logoff. Isso é feito apenas para máquinas em estado de drenagem e não para todas as máquinas ligadas. Para evitar a potencial perda de dados causada pelo logoff forçado de usuários, você pode configurar este recurso para apenas enviar lembretes de logoff sem forçar o logoff do usuário.

Você tem as seguintes opções:

- **Notificar e forçar o logoff do usuário**
- **Enviar lembretes de logoff sem forçar o logoff do usuário**
- **Nem notificar nem forçar o logoff do usuário**

Notificar e forçar o logoff do usuário

Se selecionado, o Autoscale desconecta os usuários de suas sessões após os horários especificados abaixo.



Habilitar logoff forçado durante horários de pico. Se selecionado, o Autoscale desconecta esses usuários de suas sessões durante os horários de pico quando o tempo especificado expira.

Habilitar logoff forçado durante horários de menor movimento. Se selecionado, o Autoscale desconecta esses usuários de suas sessões durante os horários de menor movimento quando o tempo especificado expira.

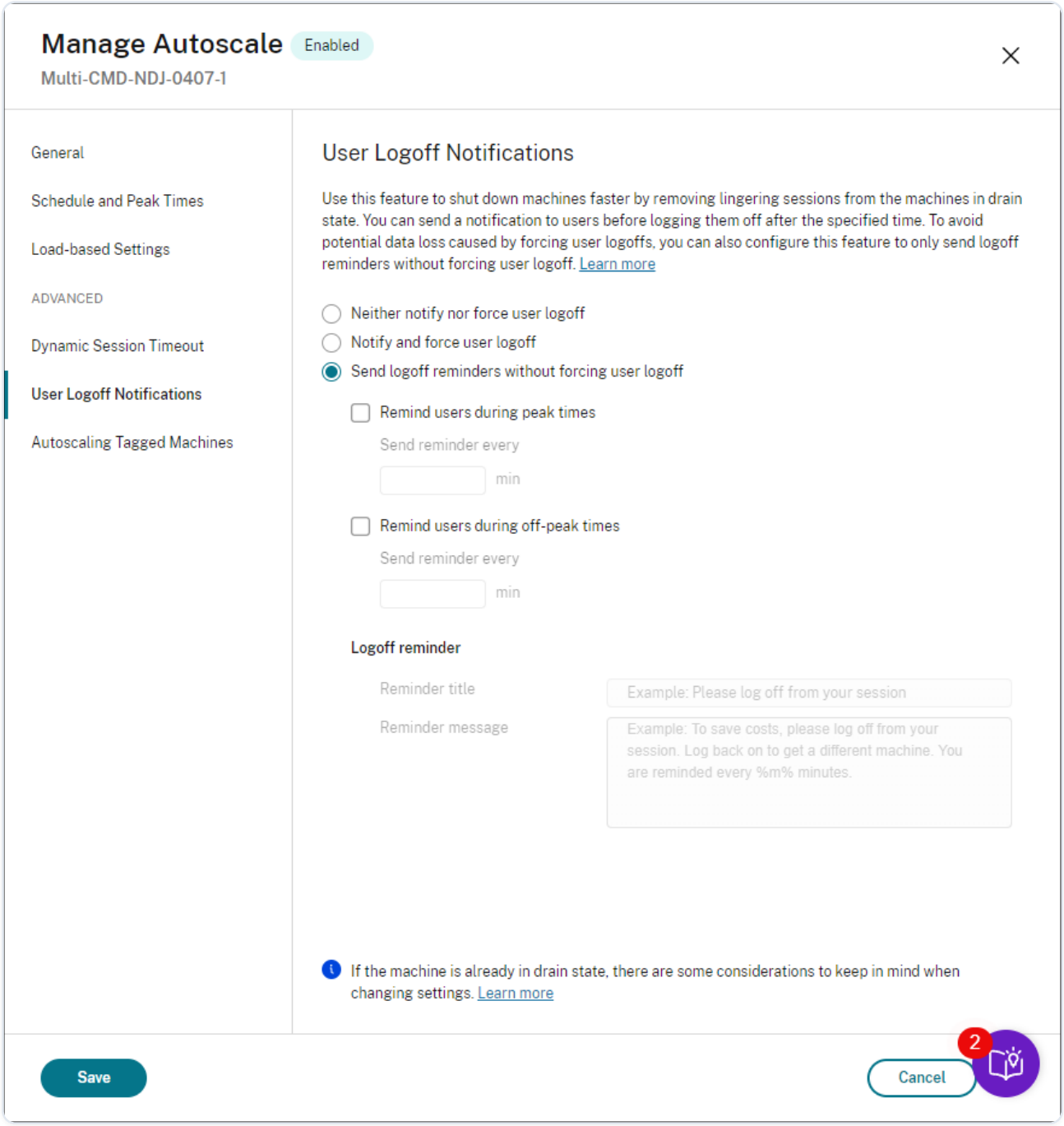
Exibir notificação depois que a máquina entrar no estado de drenagem. Permite que você envie notificações aos usuários depois que a máquina deles entrar no estado de drenagem.

- **Título da notificação**. Permite que você especifique um título para a notificação a ser enviada aos usuários. Exemplo: `A forced logoff has been initiated.`.

- **Mensagem de notificação**. Permite especificar o conteúdo da notificação a ser enviada aos usuários. Você pode usar %s% ou %m% como variáveis para indicar o tempo especificado na mensagem. Para expressar o tempo em segundos, use %s%. Para expressar o tempo em minutos, use %m%. Exemplo: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

Enviar lembretes de logoff sem forçar o logoff do usuário

Se selecionado, os usuários receberão um lembrete para fazer logoff de sua máquina depois que ela entrar no estado de drenagem. Este lembrete pode ser configurado para ser enviado no intervalo especificado abaixo.



Lembrar usuários durante horários de pico. Se selecionado, os usuários recebem um lembrete para fazer logoff de suas sessões durante os horários de pico a cada X minutos (X denota o tempo especificado).

Lembrar usuários durante horários de menor movimento. Se selecionado, os usuários recebem um lembrete para fazer logoff de suas sessões durante os horários de menor movimento a cada X minutos (X denota o tempo especificado).

Lembrete de logoff. Permite configurar o lembrete enviado aos usuários depois que a máquina deles entra no estado de drenagem.

- **Título do lembrete**. Permite especificar um título para o lembrete a ser enviado aos usuários. Exemplo: `Please log off from your session`.
- **Mensagem do lembrete**. Permite especificar uma mensagem a ser enviada aos usuários. Exemplo: `Please log off from your session and log back on to save costs`.

Não notificar nem forçar o logoff do usuário

Se selecionado, o Autoscale não força os usuários a fazer logoff de máquinas em estado de drenagem nem os notifica para mudar manualmente para uma máquina diferente.

Considerações

Se a máquina já estiver em estado de drenagem, considere o seguinte ao alterar as configurações:

- Se você alterar a configuração de **Enviar lembretes de logoff sem forçar o logoff do usuário** para **Notificar e forçar o logoff do usuário**, a nova configuração entra em vigor imediatamente.
- Se você alterar a configuração de **Notificar e forçar o logoff do usuário** para **Enviar lembretes de logoff sem forçar o logoff do usuário**, a nova configuração não entrará em vigor até a próxima vez que a máquina entrar no estado de drenagem. O usuário ainda é forçado a fazer logoff.

Analisar a eficácia das configurações do Autoscale™

Para usar este recurso, ative o botão **Autoscale Insights** em **DaaS > Início > Recursos de visualização**. Pode levar cerca de 15 minutos para que o **Autoscale Insights** apareça após a ativação.

Você pode analisar a eficácia das configurações do Autoscale com base no uso da máquina da semana anterior. Através da análise, você pode obter estas informações sobre a eficácia das configurações do Autoscale:

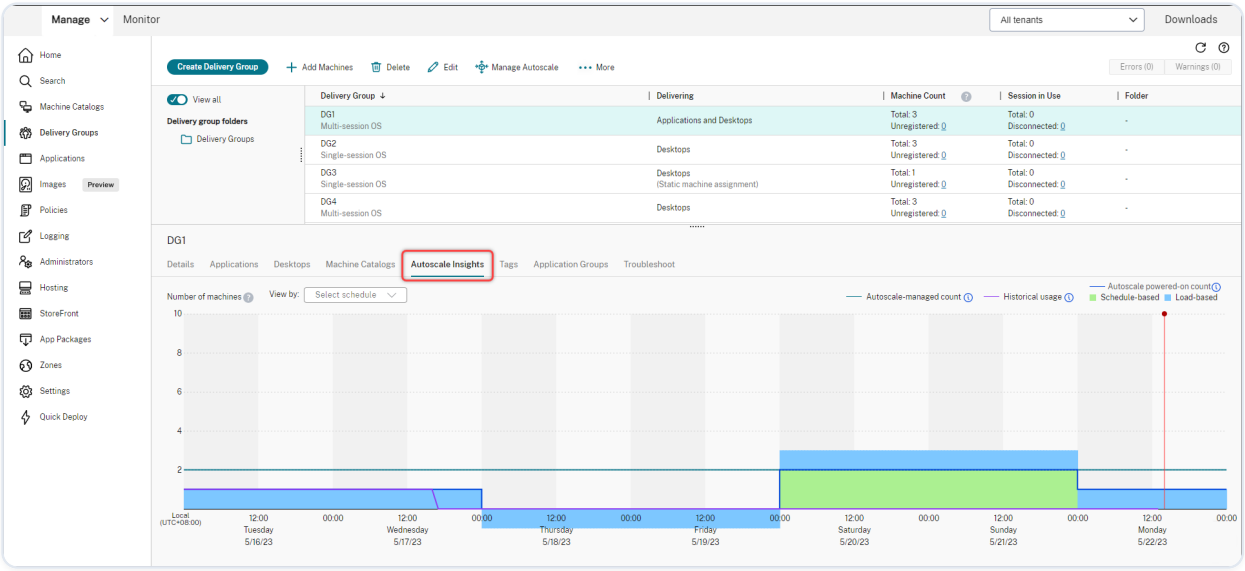
- Identificar o desperdício financeiro resultante do superprovisionamento.
- Determinar se a experiência do usuário é negativamente impactada devido ao subprovisionamento.
- Garantir que a capacidade provisionada esteja devidamente alinhada com o uso da máquina.

Para atingir este objetivo, siga estes passos:

1. Selecione um grupo de entrega com Autoscale ativado.

2. No painel inferior, clique na guia **Autoscale Insights**.

   O gráfico a seguir aparece, mostrando a comparação entre os dados de uso da máquina da semana anterior e o número de máquinas a serem ligadas com base nas configurações do Autoscale.



* A linha vertical vermelha identifica a hora atual.

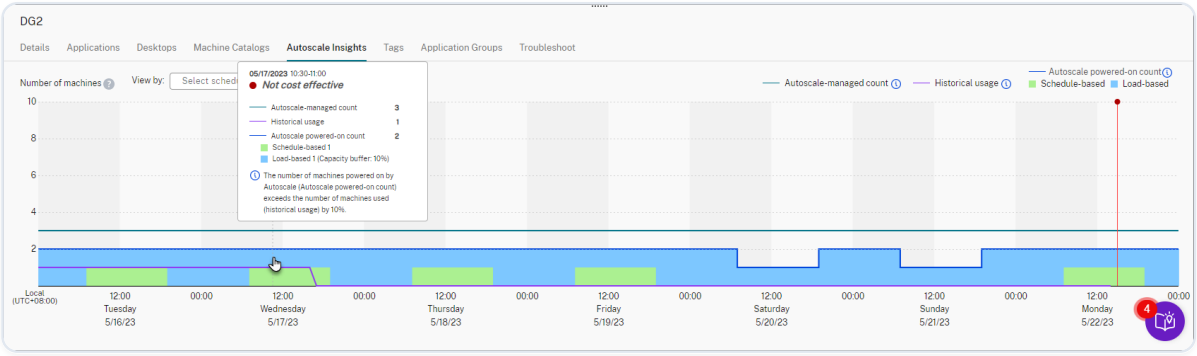
A tabela a seguir fornece descrições das métricas mostradas neste gráfico.

MÉTRICA	DESCRIÇÃO
Contagem gerenciada pelo Autoscale	Número total de máquinas gerenciadas pelo Autoscale. Contagem gerenciada pelo Autoscale = Número total de máquinas no grupo de entrega – Número de máquinas em modo de manutenção – Número de máquinas não marcadas para Autoscale (Se o recurso Autoscale marcado estiver ativado).
Contagem de máquinas ligadas pelo Autoscale	Número total de máquinas ligadas pelo Autoscale. Contagem de máquinas ligadas pelo Autoscale = Contagem de máquinas baseada em agendamento + Contagem de máquinas baseada em carga.
Uso histórico	Número de máquinas que foram entregues aos usuários.

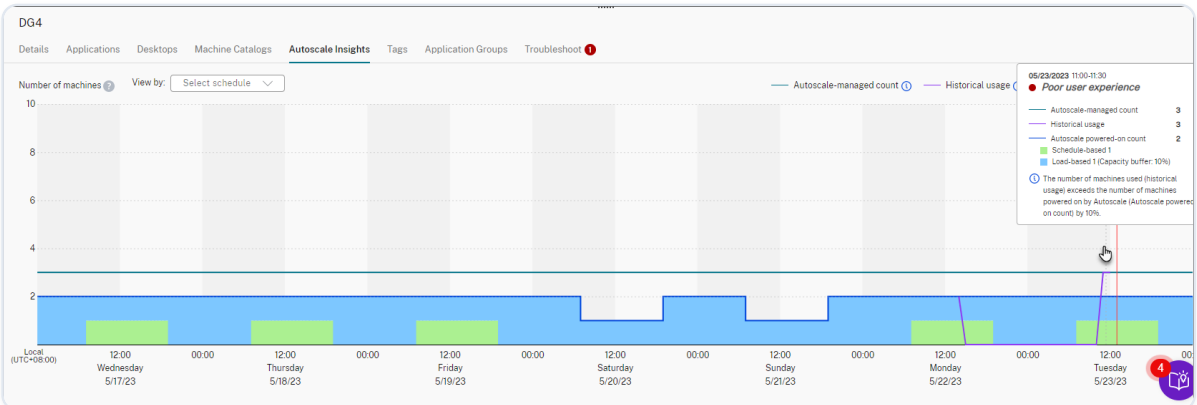
MÉTRICA	DESCRIÇÃO
Baseado em agendamento	Número de máquinas que são ligadas com base nas configurações de agendamento do Autoscale (**Observação:** As configurações baseadas em agendamento não se aplicam a grupos de entrega do tipo OS de sessão única estática).
Baseado em carga	Número de máquinas que são ligadas com base nas configurações de carga do Autoscale.

3. Para verificar a eficácia das configurações do Autoscale em um determinado período, passe o mouse sobre esse período no gráfico. Uma caixa de informações é exibida, mostrando os resultados da comparação e as contagens detalhadas de máquinas:

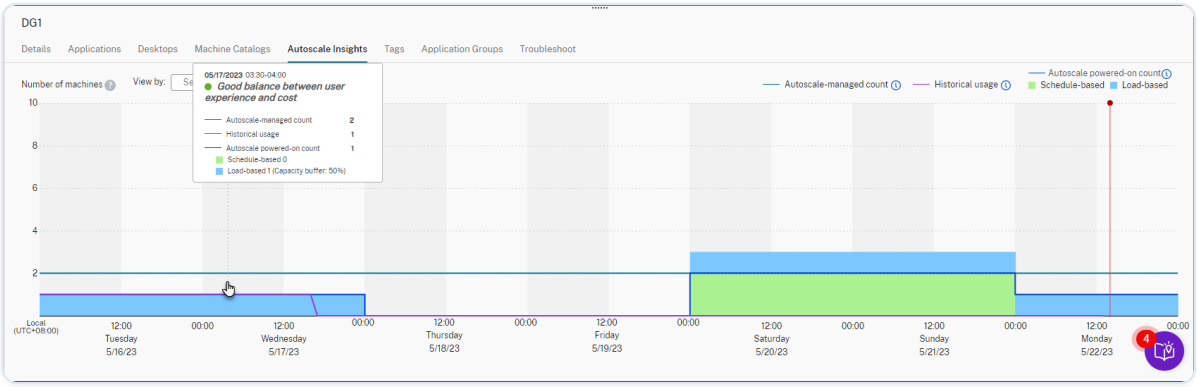
   - **Não é econômico**. O uso histórico é inferior a 90% das configurações do Autoscale (contagem de máquinas ligadas pelo Autoscale). Como resultado, pode haver capacidade desperdiçada.



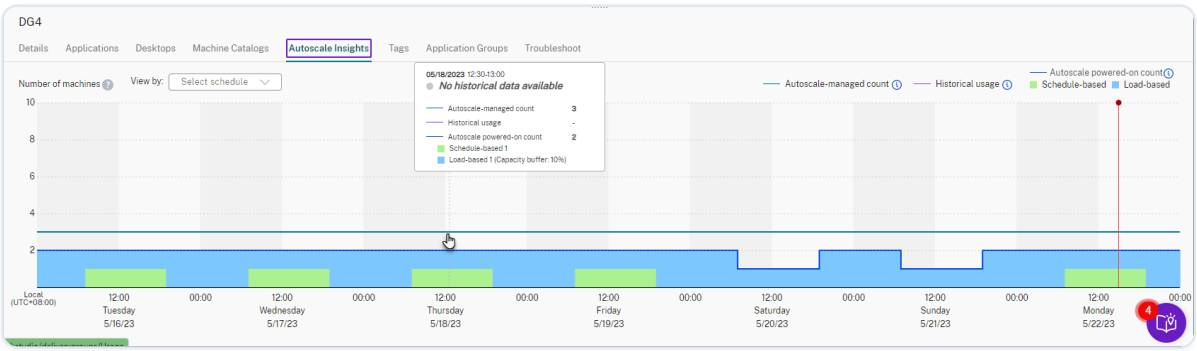
   - **Experiência do usuário ruim**. O uso histórico é superior a 110% das configurações do Autoscale (contagem de máquinas ligadas pelo Autoscale). Como resultado, os usuários podem experimentar tempos de espera mais longos para que as máquinas liguem.



- **Bom equilíbrio entre experiência do usuário e custo**. A diferença entre o uso histórico e as configurações do Autoscale (contagem de máquinas ligadas pelo Autoscale) é inferior a 10%. As configurações do Autoscale estão alinhadas com o uso histórico.



- **Nenhum dado histórico disponível**. Nenhum dado histórico está disponível. As possíveis causas incluem o Autoscale ter sido habilitado para o grupo de entrega há menos de uma semana.



4. Para destacar um intervalo de datas com base em um agendamento do Autoscale, selecione o agendamento no campo **Exibir por**.
5. Com base na sua análise, ajuste as configurações do Autoscale. Para obter mais informações, consulte Configurações baseadas em agendamento e carga.

Comandos do SDK do Broker PowerShell

Você pode configurar o Autoscale para grupos de entrega usando o SDK do Broker PowerShell. Para configurar o Autoscale usando comandos PowerShell, você deve usar a versão 7.21.0.12 ou posterior do SDK do Remote PowerShell. Para obter mais informações sobre o SDK do Remote PowerShell, consulte SDKs e APIs.

Set-BrokerDesktopGroup

Desabilita ou habilita um BrokerDesktopGroup existente ou altera suas configurações

Para obter mais informações sobre este cmdlet, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`.

EXEMPLOS

Consulte os exemplos a seguir para obter detalhes sobre como usar os cmdlets do PowerShell.

Habilitar Autoscale™:

- Suponha que você queira habilitar o Autoscale para o grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

Configurar o buffer de capacidade separadamente para horários de pico e fora de pico:

- Suponha que você queira definir o buffer de capacidade para 20% para horários de pico e 10% para horários fora de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

Configurar a definição de *tempo limite de desconexão*:

- Suponha que você queira definir o valor de **tempo limite de desconexão** para 60 minutos para horários de pico e 30 minutos para horários fora de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

Configurar a configuração de *tempo limite quando desconectado*:

- Suponha que você queira definir o valor de **tempo limite quando desconectado** para 60 minutos para horários de pico e 30 minutos para horários fora de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

Configurar a configuração de *atraso de desligamento*:

- Suponha que você queira definir o atraso de desligamento para 15 minutos para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

Configurar um período de tempo durante o qual o atraso de desligamento não entra em vigor:

- Suponha que você queira que o atraso de desligamento entre em vigor até que 30 minutos tenham decorrido para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`.

Configurar a configuração de *custo da instância da máquina*:

- Suponha que você queira definir o custo da instância da máquina por hora para 0,2 dólares para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

Excluir VMs em modo de manutenção do pool de autoscale:

- Considere um grupo de entrega com 10 máquinas, das quais 2 máquinas estão em modo de manutenção. A capacidade do buffer do Autoscale é definida como 50%. Suponha que, se você quiser excluir as VMs em modo de manutenção do pool de autoscale, defina `PoolSizeExcludesMaintenanceMode` como `True`. O Autoscale então inicia 4 máquinas, pois as 2 máquinas em modo de manutenção não estão incluídas no pool de máquinas. Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

  ```
  PS C:\> Set-BrokerDesktopGroup -PoolSizeExcludesMaintenanceMode $true
  ```

  O valor padrão para `PoolSizeExcludesMaintenanceMode` para os grupos de entrega de sessão única é `False`.

  O valor padrão para `PoolSizeExcludesMaintenanceMode` para os grupos de entrega de múltiplas sessões é `True`.

New-BrokerPowerTimeScheme

Cria um BrokerPowerTimeScheme para um grupo de entrega. Para obter mais informações, consulte `<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`.

Exemplo

Suponha que você queira criar um esquema de tempo de energia para um grupo de entrega cujo valor UID é 3. O novo esquema abrange o fim de semana, segunda e terça-feira. O período das 8:00 AM às 6:30 PM é definido como horários de pico para os dias incluídos no esquema. Para horários de pico, o tamanho do pool (o número de máquinas mantidas ligadas) é 20. Para horários fora de pico, é 5. Você pode usar o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

Parâmetros para tempos limite de sessão dinâmicos

Os seguintes cmdlets do SDK do Broker PowerShell foram estendidos para tempos limite de sessão dinâmicos, suportando múltiplos novos parâmetros:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Esses parâmetros incluem:

- **DisconnectPeakIdleSessionAfterSeconds** – Representa o tempo em segundos após o qual uma sessão ociosa é desconectada durante o horário de pico. Esta propriedade tem um valor padrão de 0, o que indica a desativação de seu comportamento associado durante o horário de pico. Um valor maior que 0 habilita seu comportamento para o grupo de entrega apenas durante o horário de pico.
- **DisconnectOffPeakIdleSessionAfterSeconds** - Representa o tempo em segundos após o qual uma sessão ociosa é desconectada durante o horário de folga. O valor padrão desta

propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário de folga. Um valor maior que 0 habilita seu comportamento associado para o grupo de entrega apenas durante o horário de folga.

- **LogoffPeakDisconnectedSessionAfterSeconds** - Representa o tempo em segundos após o qual uma sessão desconectada é encerrada durante o horário de pico. O valor padrão desta propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário de pico. Um valor maior que 0 habilita seu comportamento associado para o grupo de entrega apenas durante o horário de pico.
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - Representa o tempo em segundos após o qual uma sessão desconectada é encerrada durante o horário de folga. O valor padrão desta propriedade é 0, o que indica a desativação de seu comportamento associado durante o horário de folga. Um valor maior que 0 habilita seu comportamento associado para o grupo de entrega apenas durante o horário de folga.

Exemplo

Suponha que você queira definir o tempo limite de sessão ociosa para 3.600 segundos durante os horários de pico para um grupo de entrega cujo nome é "MyDesktop". Use o comando PowerShell `Set-BrokerDesktopGroup`. Por exemplo:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

Fazer isso desconecta as sessões que ficaram ociosas por mais de 1 hora no horário de folga para o grupo de desktop cujo nome é "MyDesktop".

Verificação de Integridade da Nuvem

> **Nota:**
>
> O Cloud Health Check está integrado ao Citrix DaaS. A integração está disponível como a ação Executar Verificação de Integridade no Studio. Para obter mais informações, consulte Solucionar problemas de registro de VDA e inicialização de sessão.

> O Cloud Health Check permite executar verificações que avaliam a integridade e a disponibilidade do site e seus componentes. Você pode executar verificações de integridade para Virtual Delivery Agents (VDAs), servidores StoreFront™ e Profile Management. As

> verificações de integridade de VDA identificam possíveis causas para problemas comuns de registro de VDA e inicialização de sessão.

Se houver problemas durante as verificações, o Cloud Health Check fornece um relatório detalhado e as ações para corrigir os problemas. Cada vez que o Cloud Health Check é iniciado, ele verifica a versão mais recente dos scripts na Content Delivery Network (CDN) e os baixa automaticamente se não existirem na máquina local. O Cloud Health Check sempre escolhe a versão local mais recente dos scripts para executar as verificações de integridade.

> **Nota:**
>
> O Cloud Health Check não é atualizado toda vez que é executado.

> Em um ambiente Citrix Cloud™, execute o Cloud Health Check a partir de uma máquina ingressada no domínio para executar verificações em um ou mais VDAs ou servidores StoreFront.

> **Nota:**
>
> Você não pode instalar ou executar o Cloud Health Check em um Cloud Connector.

> O log do aplicativo Cloud Health Check é armazenado em `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`. Você pode usar este arquivo para solucionar problemas.

Veja uma introdução ao Cloud Health Check.



Veja quando usar o Cloud Health Check.



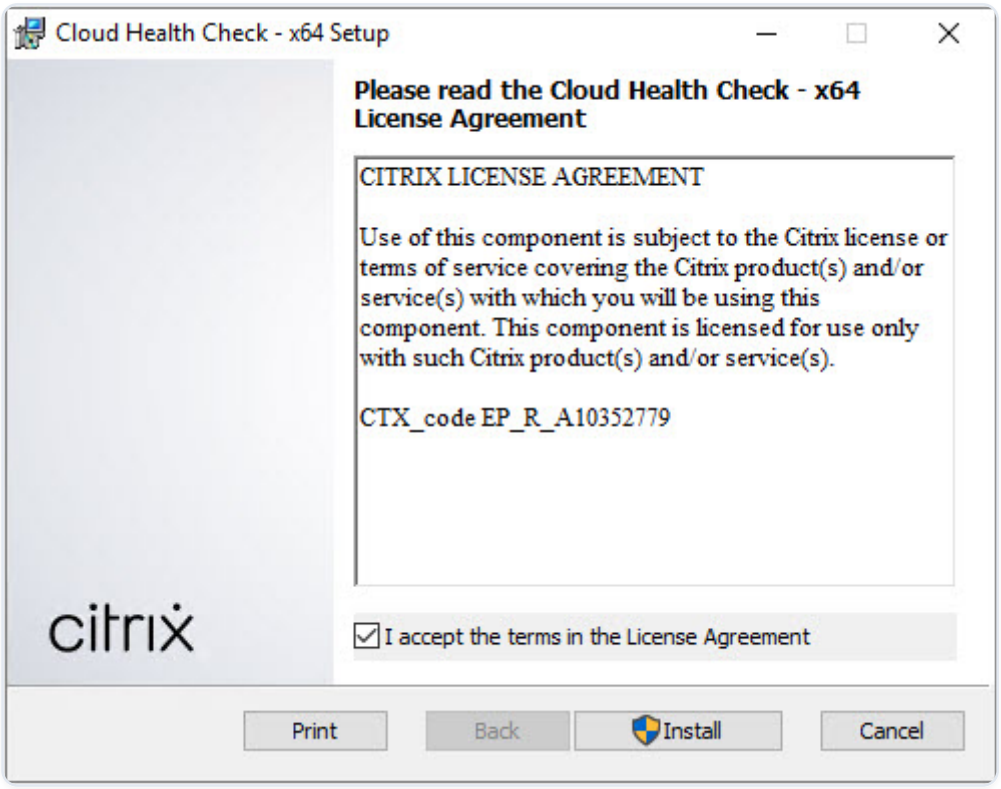
Instalação

Para preparar seu ambiente para a instalação do Cloud Health Check, você deve ter uma máquina Windows ingressada no domínio.

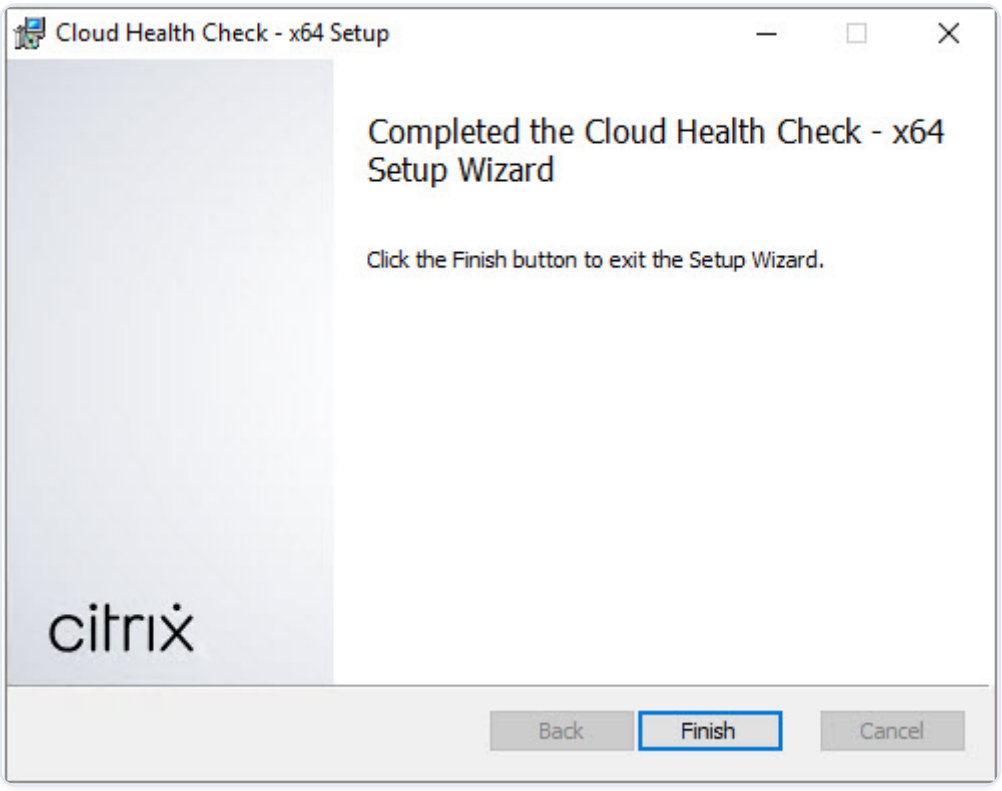
Nota:

Você não pode instalar ou executar o Cloud Health Check no Cloud Connector.

1. Na máquina ingressada no domínio, baixe o instalador do Cloud Health Check.
2. Clique duas vezes no arquivo CloudHealthCheckInstaller_x64.msi.
3. Marque a caixa para aceitar os termos.
4. Clique em Instalar.



5. Após a conclusão da instalação, clique em **Concluir**.



Permissões e requisitos

Permissões:

- Para executar verificações de integridade:
  - Você deve ser membro do grupo de usuários do domínio.
  - Você deve ser um administrador completo ou ter uma função personalizada com permissões de somente leitura e **Executar Testes de Ambiente** para o site.
  - Defina a política de execução de script para pelo menos `RemoteSigned` para permitir que os scripts sejam executados. Por exemplo: `Set-ExecutionPolicy RemoteSigned`. **Observação:** outras permissões de execução de script também podem funcionar.
- Use **Executar como administrador** ao iniciar o Cloud Health Check.

Para cada máquina VDA ou StoreFront na qual você executa verificações de integridade:

- O SO deve ser de 64 bits.
- A máquina deve estar ingressada na mesma floresta de domínio do Active Directory que o host da verificação de integridade.
- O Cloud Health Check deve ser capaz de se comunicar com a máquina.
- O compartilhamento de arquivos e impressoras deve estar ativado.

- PSRemoting e WinRM devem estar habilitados. A máquina também deve estar executando o PowerShell 3.0 ou posterior.
- O acesso à Windows Management Infrastructure (WMI) deve estar habilitado na máquina.

Sobre as verificações de integridade

Os dados da verificação de integridade são armazenados em pastas em `C:\ProgramData\Citrix\TelemetryService\`.

Verificações de integridade do VDA

Para registro no VDA, o Cloud Health Check verifica:

- Instalação do software VDA
- Associação de domínio da máquina VDA
- Disponibilidade da porta de comunicação do VDA
- Status do serviço VDA
- Configuração do firewall do Windows
- Comunicação com o Controller
- Sincronização de tempo com o Controller
- Status de registro do VDA

Para inicializações de sessão em VDAs, o Cloud Health Check verifica:

- Disponibilidade da porta de comunicação de inicialização da sessão
- Status dos serviços de inicialização da sessão
- Configuração do firewall do Windows para inicialização da sessão
- Licenças de Acesso para Cliente dos Serviços de Área de Trabalho Remota do VDA
- Caminho de inicialização do aplicativo VDA
- Configurações de registro de inicialização da sessão
- Status do Citrix Universal™ Injection Driver (CTXUVI)

Para o Profile Management em VDAs, o Cloud Health Check verifica:

- Detecção de hipervisor
- Detecção de provisionamento
- Citrix Aplicativos Virtuais e Desktops™

- Configuração de vDisk pessoal
- Repositório de usuário
- Detecção de status do serviço Profile Management
- Teste de hooking do Winlogon.exe

Para executar verificações no Profile Management, você deve instalar e habilitar o Profile Management no VDA. Para obter mais informações sobre as verificações de configuração do Profile Management, consulte o artigo da Central de Conhecimento CTX132805.

Verificações de integridade do StoreFront

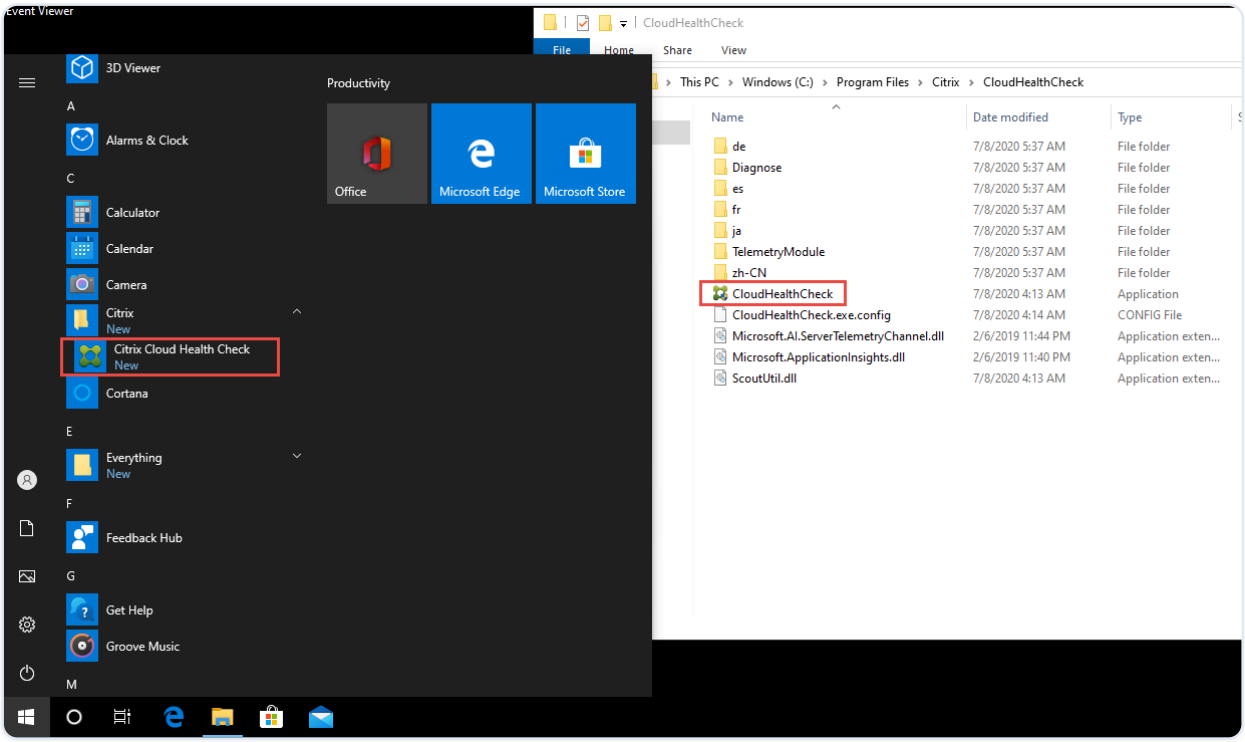
As verificações do StoreFront verificam se:

- O serviço Citrix Default Domain está em execução
- O serviço Citrix Credential Wallet está em execução
- A conexão do servidor StoreFront com o Active Directory é a porta 88
- A conexão do servidor StoreFront com o Active Directory é a porta 389
- A conexão do servidor StoreFront com o Active Directory é a porta 464
- A URL base tem um FQDN válido
- O endereço IP correto da URL base pode ser recuperado
- O pool de aplicativos do IIS está usando .NET 4.0
- O certificado está vinculado à porta SSL para a URL do host
- A cadeia de certificados está completa
- Os certificados expiraram
- Um certificado está expirando em 30 dias

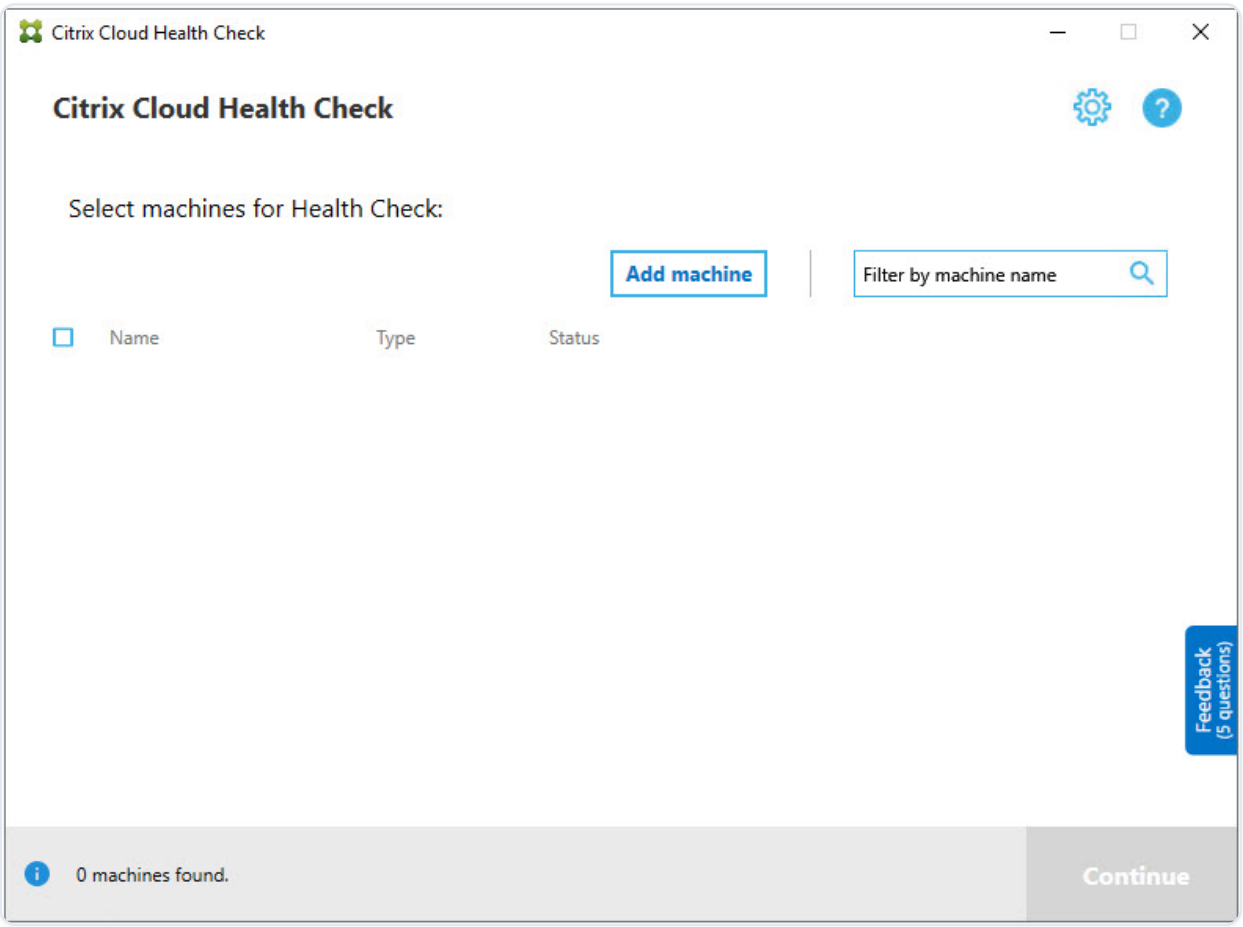
Executando o Cloud Health Check

Para executar o Citrix Cloud Health Check:

1. Selecione **Citrix > Citrix Cloud Health Check** no menu Iniciar da máquina, ou execute `CloudHealthCheck.exe` em `C:\Program Files\Citrix\CloudHealthCheck`.

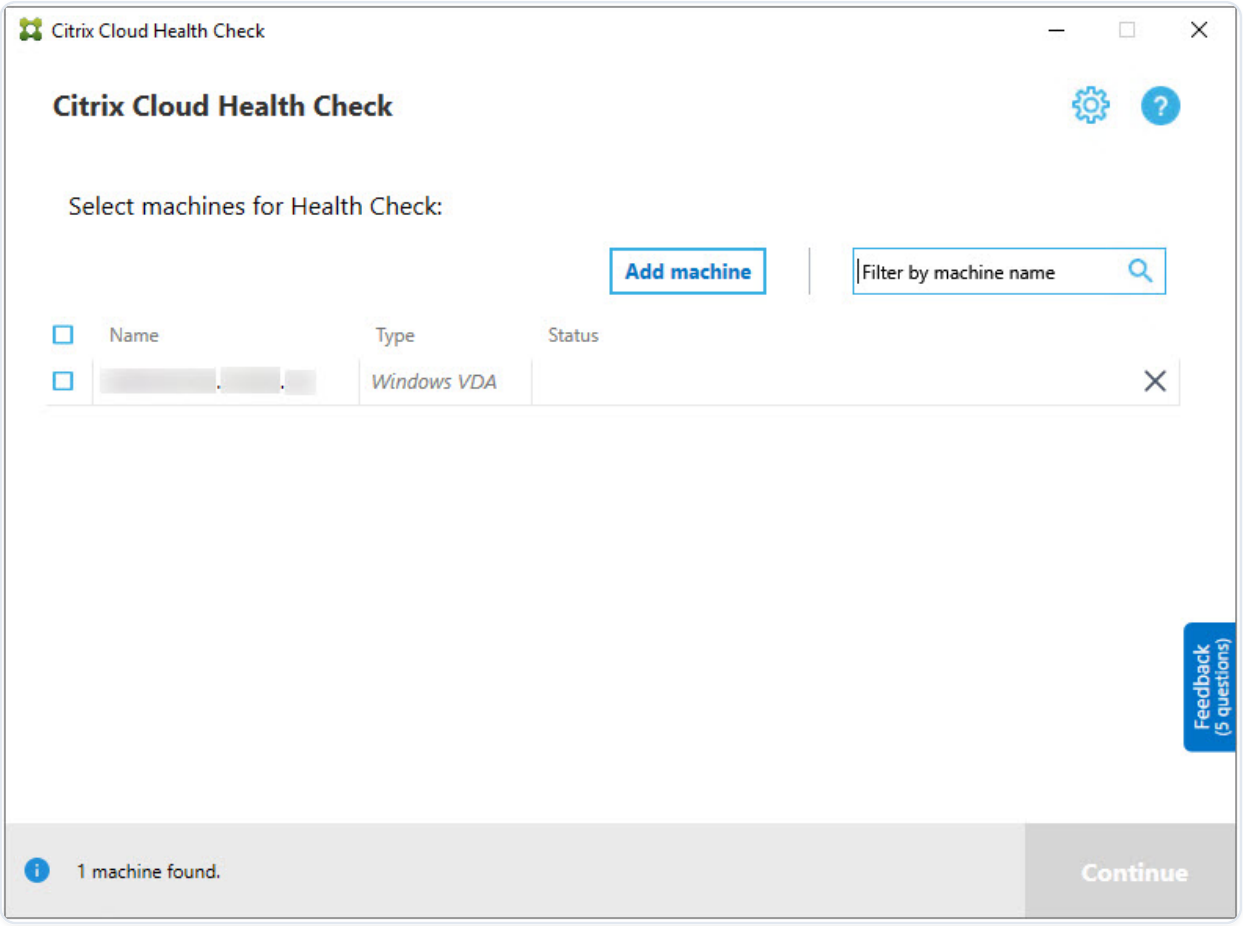


2. Na tela principal do Cloud Health Check, clique em **Adicionar máquina**.



3. Digite o FQDN da máquina que você deseja adicionar. **Observação:** Embora inserir um alias DNS em vez de um FQDN possa parecer válido, as verificações de integridade podem falhar.
4. Clique em **Continuar**.

5. Repita para adicionar outras máquinas conforme necessário.



6. Para remover uma máquina adicionada manualmente, clique no **X** no lado direito da linha e confirme a exclusão. Repita para excluir outras máquinas adicionadas manualmente.

O Cloud Health Check lembra as máquinas adicionadas manualmente até que você as remova. Quando você fecha e reabre o Cloud Health Check, as máquinas adicionadas manualmente ainda são listadas no topo da lista.

Importar máquinas VDA

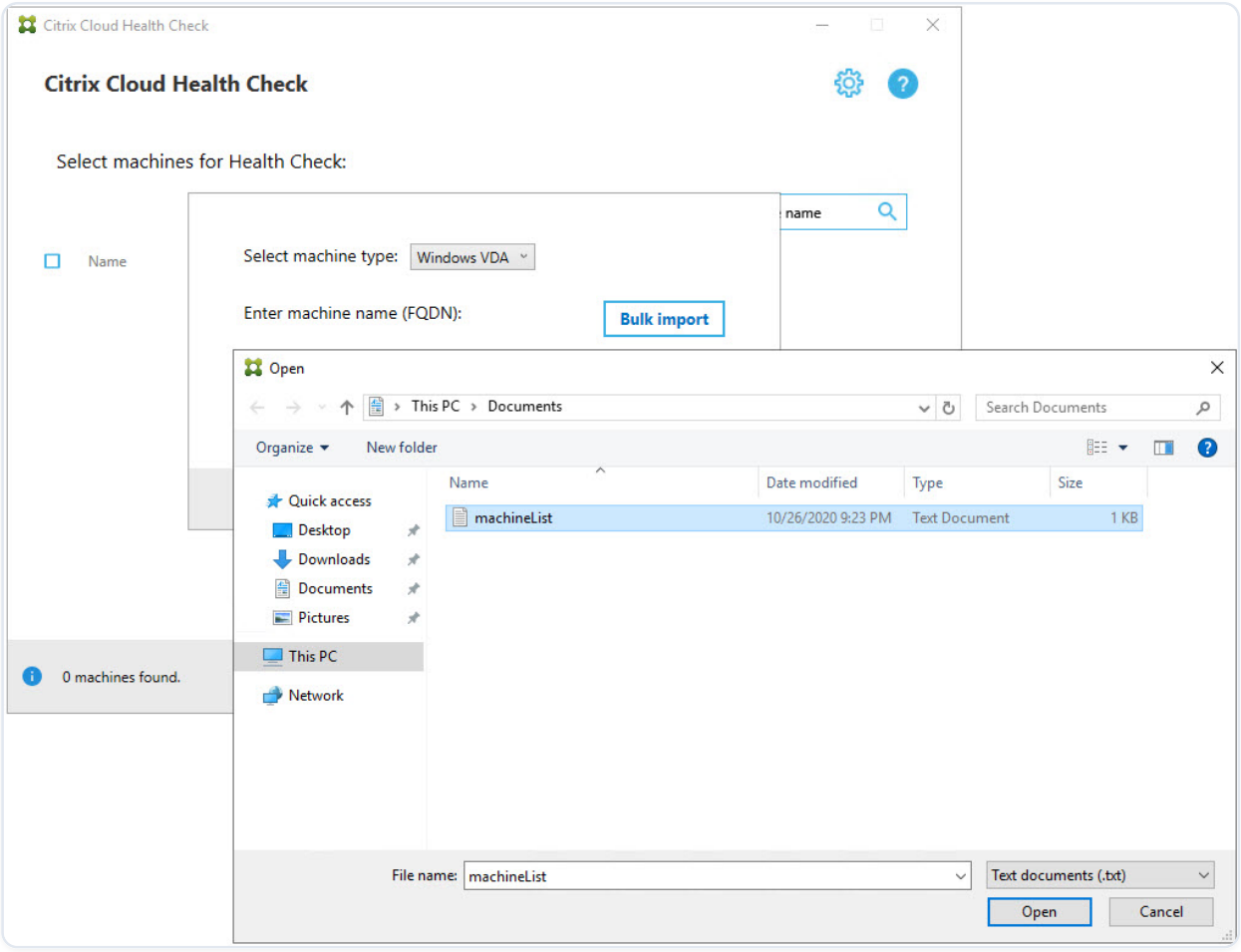
Você pode importar máquinas VDA na implantação ao executar verificações de integridade.

1. No Connector, gere o arquivo de lista de máquinas com o seguinte comando PowerShell. No Connector, você deve inserir as credenciais Citrix e selecionar o cliente na caixa de diálogo pop-up.

```
Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
```

1. Copie o arquivo machineList.txt para a máquina ingressada no domínio na qual você deseja executar o Cloud Health Check.
2. Na página do Cloud Health Check, clique em **Adicionar Máquina**.

3. Selecione o tipo de máquina VDA do Windows.
4. Clique em **Importar máquinas VDA**.
5. Selecione o arquivo machineList.txt.
6. Clique em **Abrir**.



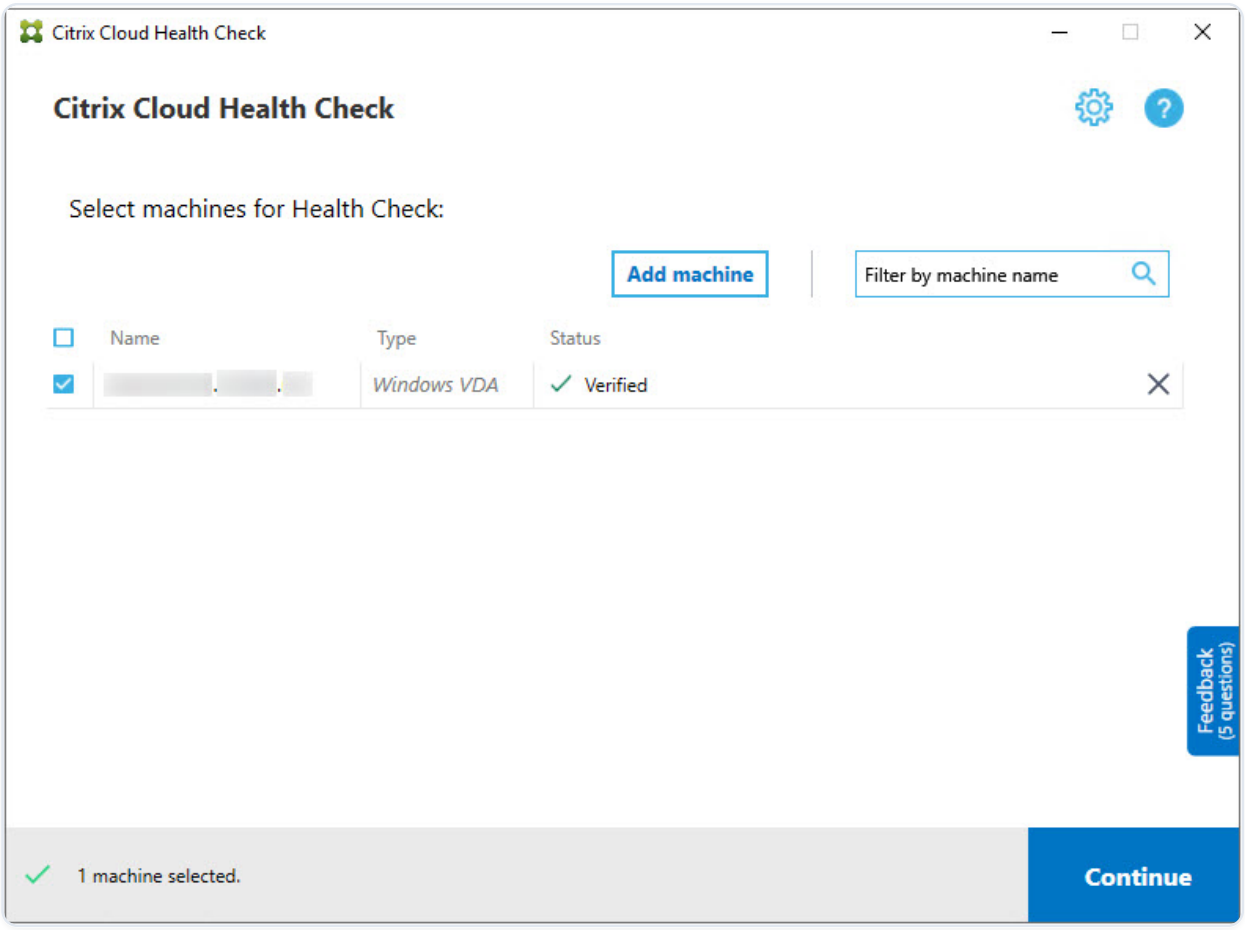
As máquinas VDA importadas são listadas na página Verificação de Integridade da Nuvem.

7. Selecione a caixa de seleção ao lado de cada máquina na qual você deseja executar verificações de integridade.

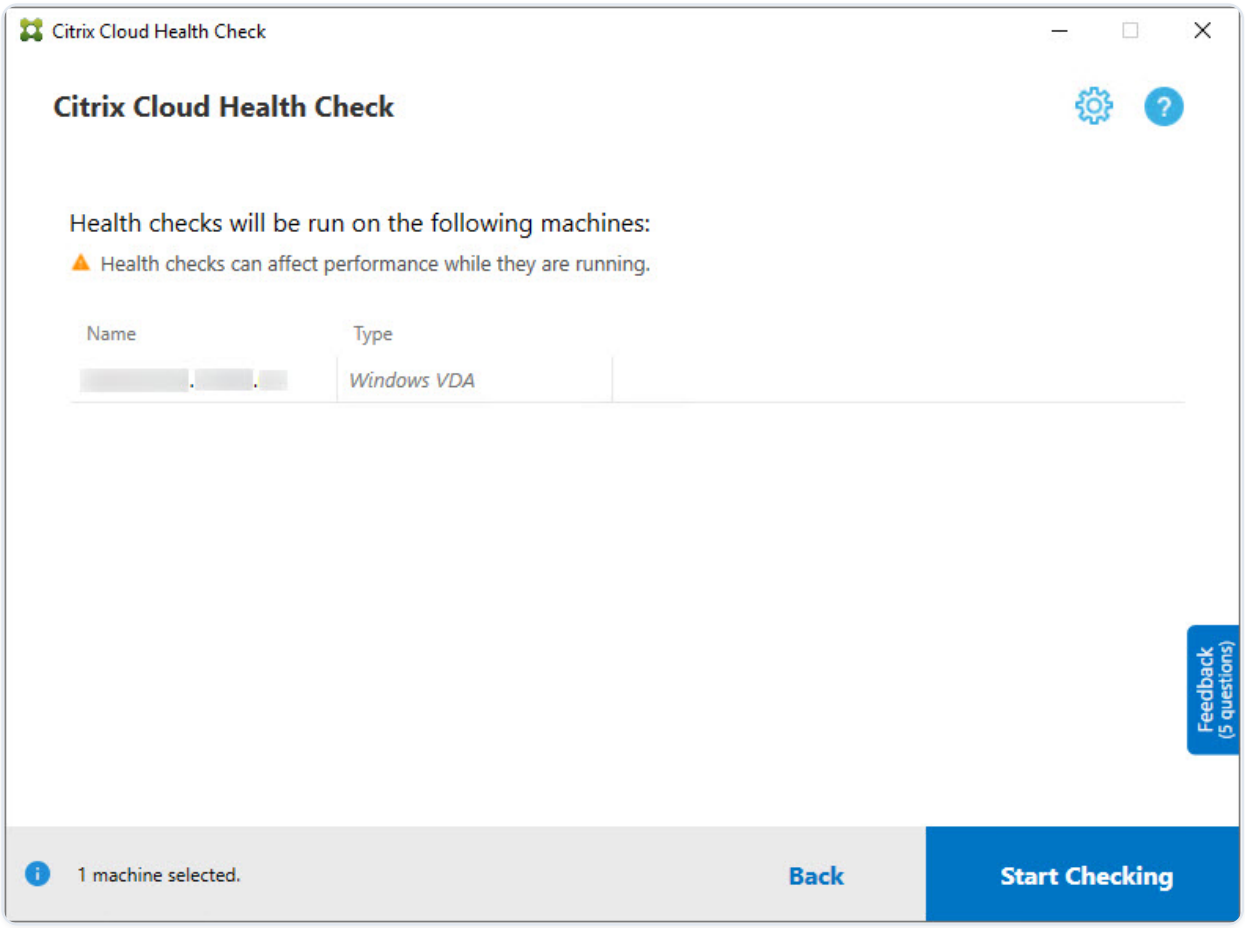
   A Verificação de Integridade da Nuvem inicia automaticamente testes de verificação em cada máquina selecionada, garantindo que ela atenda aos critérios listados nos testes de verificação. Se a verificação falhar, uma mensagem aparecerá na coluna **Status**, e a caixa de seleção dessa máquina será desmarcada. Você pode então:

   - Resolva o problema e, em seguida, selecione a caixa de seleção da máquina novamente. Isso aciona uma nova tentativa dos testes de verificação.
   - Ignore essa máquina deixando sua caixa de seleção desmarcada. As verificações de integridade não são executadas para essa máquina.

8. Quando os testes de verificação estiverem concluídos, clique em **Continuar**.

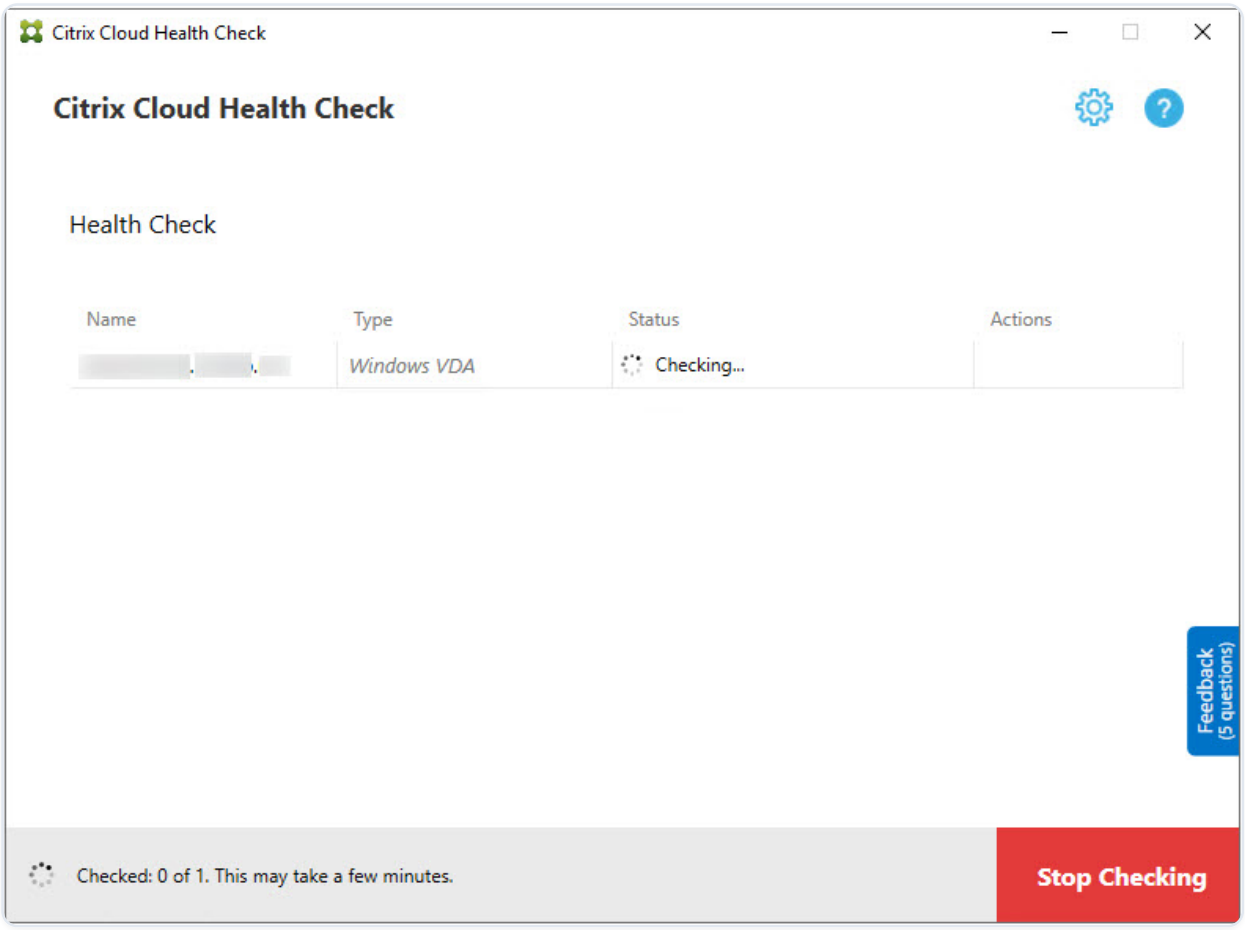


9. Execute as verificações de integridade nas máquinas selecionadas. O resumo lista as máquinas onde os testes são executados (as máquinas que você selecionou e que passaram nos testes de verificação).
10. Clique em **Iniciar Verificação**.

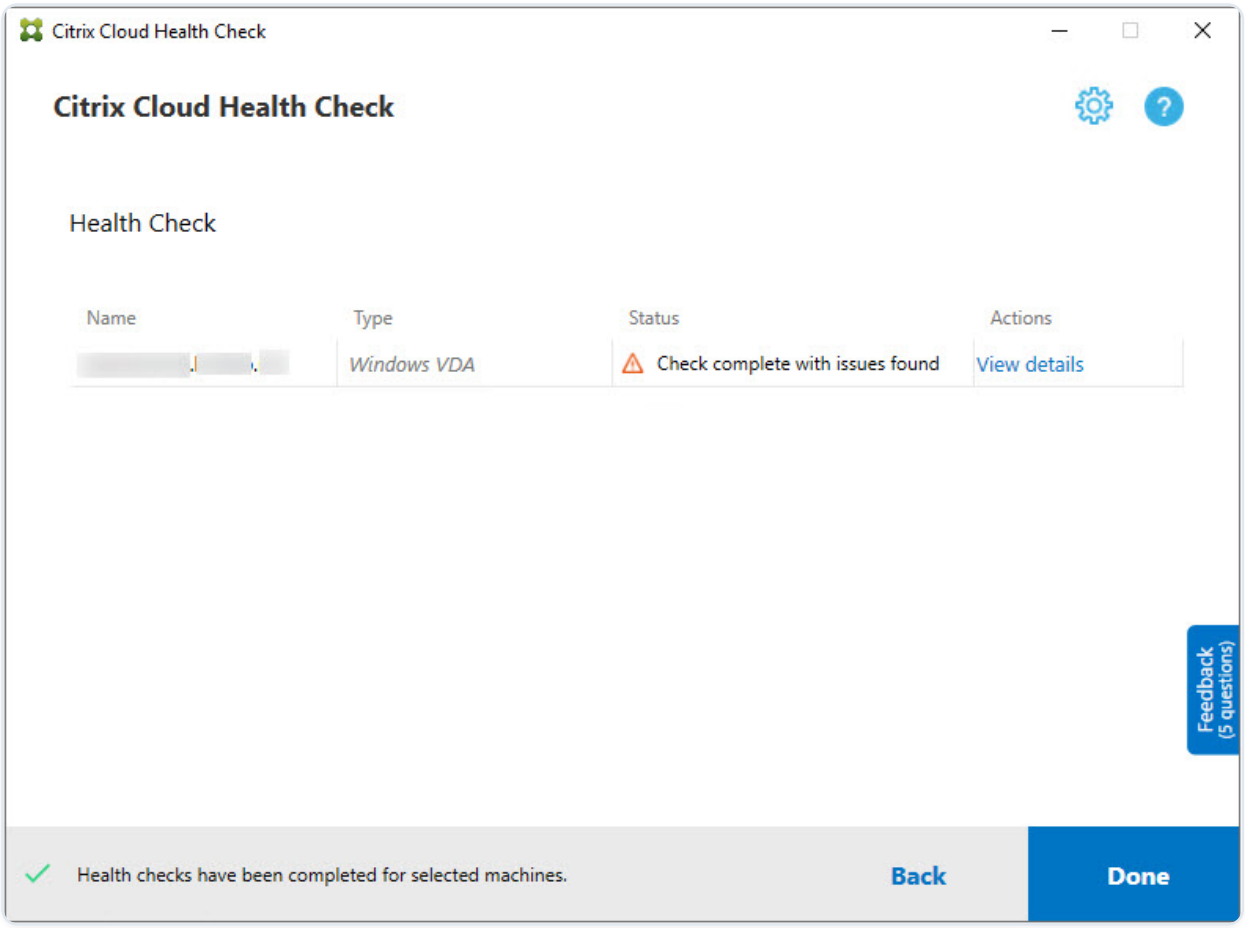


Durante e após a verificação, a coluna **Status** indica o estado de verificação atual de uma máquina.

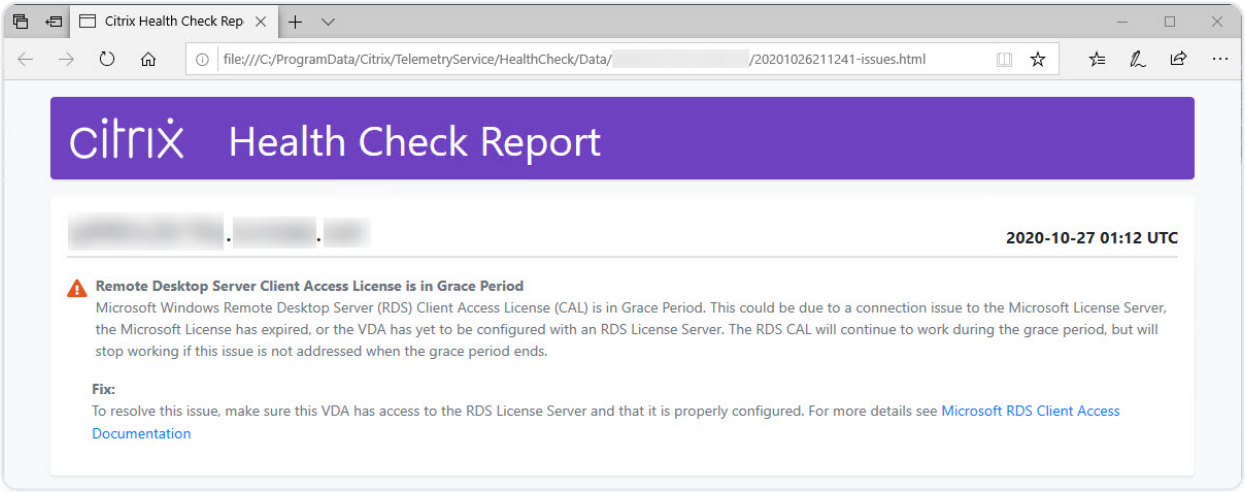
11. Para parar todas as verificações em andamento, clique em **Parar Verificação** no canto inferior direito da página. Você não pode cancelar a verificação de integridade de uma única máquina; você só pode cancelar a verificação para todas as máquinas selecionadas.



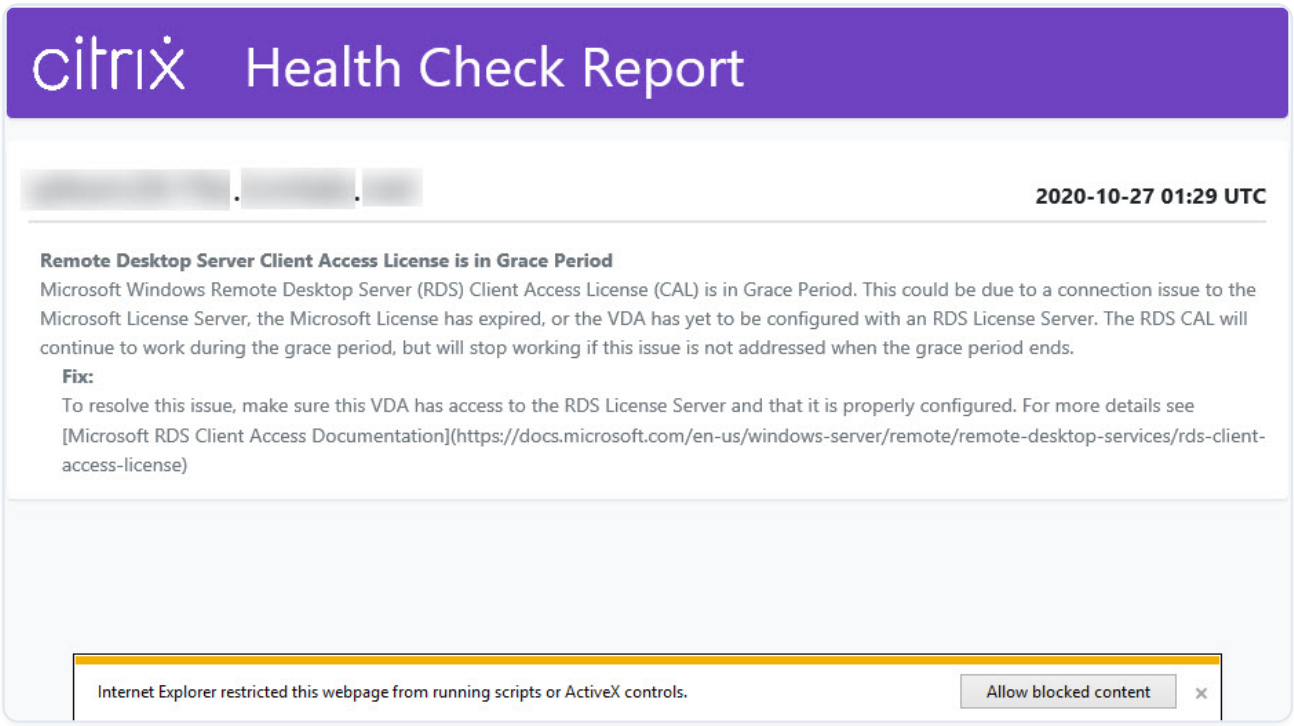
12. Quando as verificações estiverem concluídas para todas as máquinas selecionadas, o botão **Parar Verificação** no canto inferior direito muda para **Concluído**.



- Se uma verificação falhar, você pode clicar em **Tentar novamente** na coluna **Ação**.
- Se uma verificação for concluída sem problemas encontrados, a coluna **Ação** estará vazia.
- Se uma verificação encontrar problemas, clique em **Exibir detalhes** para ver os resultados.



Se você usar o Internet Explorer para visualizar o relatório, deverá clicar em **Permitir conteúdo bloqueado** para exibir o hiperlink.



Depois que a verificação for concluída para todas as máquinas selecionadas, clicar em **Voltar** fará com que você perca os resultados da verificação.

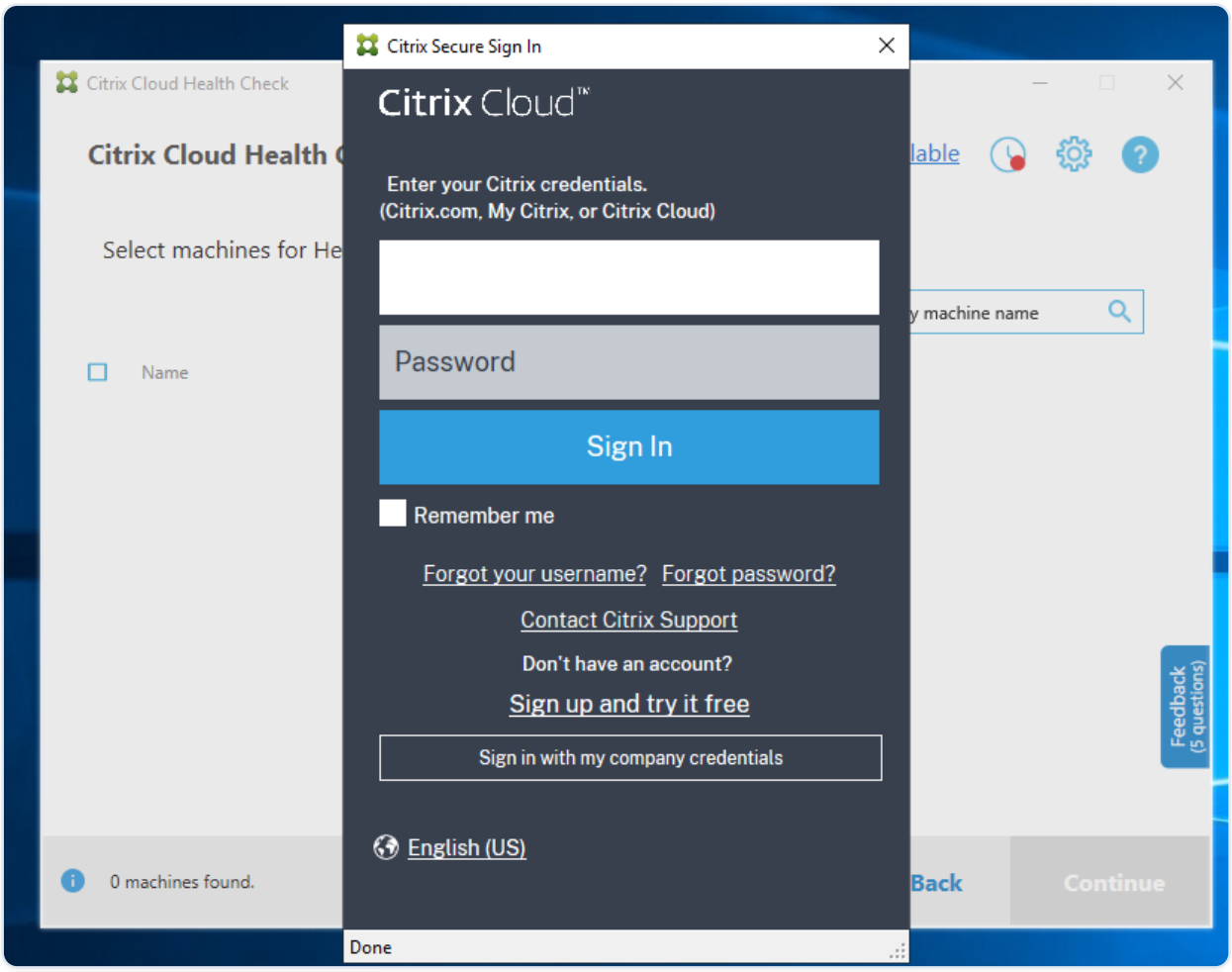
Quando as verificações forem concluídas, clique em **Concluído** para retornar à tela principal do Cloud Health Check.

Recuperar máquinas VDA

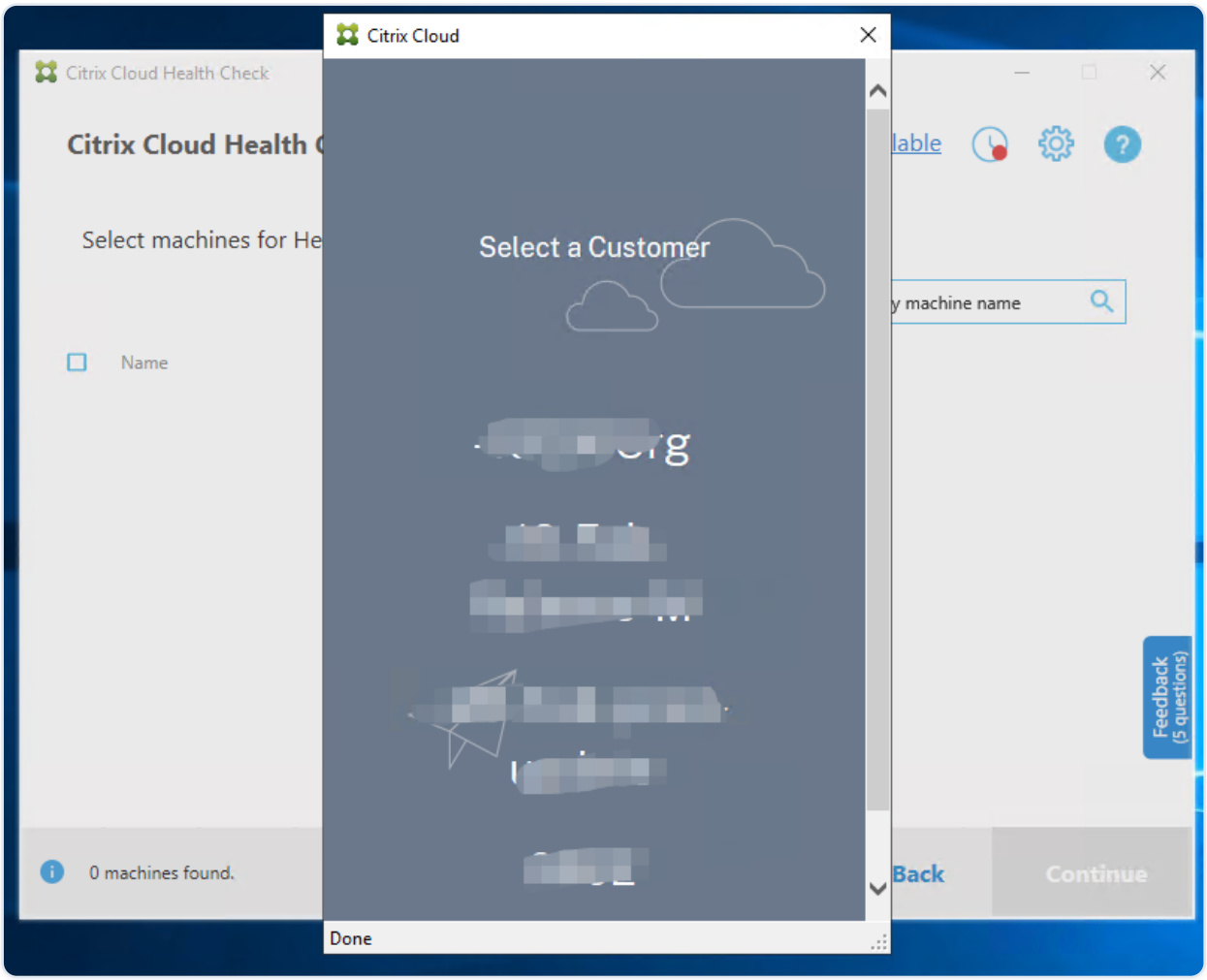
O Cloud Health Check pode detectar e recuperar VDAs automaticamente de suas implantações do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops).

Para recuperar seus VDAs:

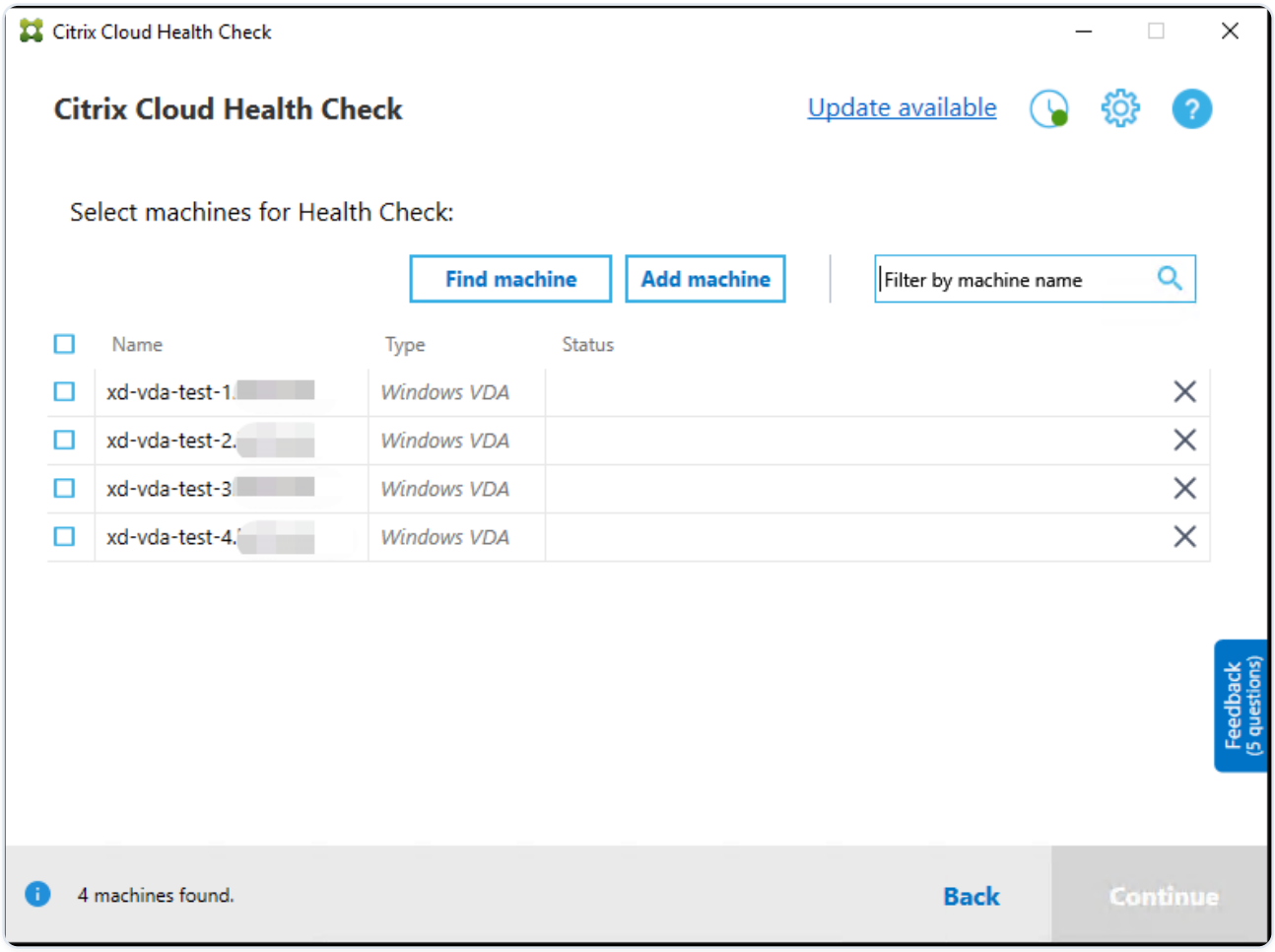
1. Prepare uma nova máquina que esteja unida à mesma floresta de domínio da máquina em que o Cloud Health Check é executado.
2. Abra o Cloud Health Check e clique em **Localizar máquina** para fazer login no Citrix Cloud.



3. Selecione o cliente com o site de nuvem que você deseja recuperar.



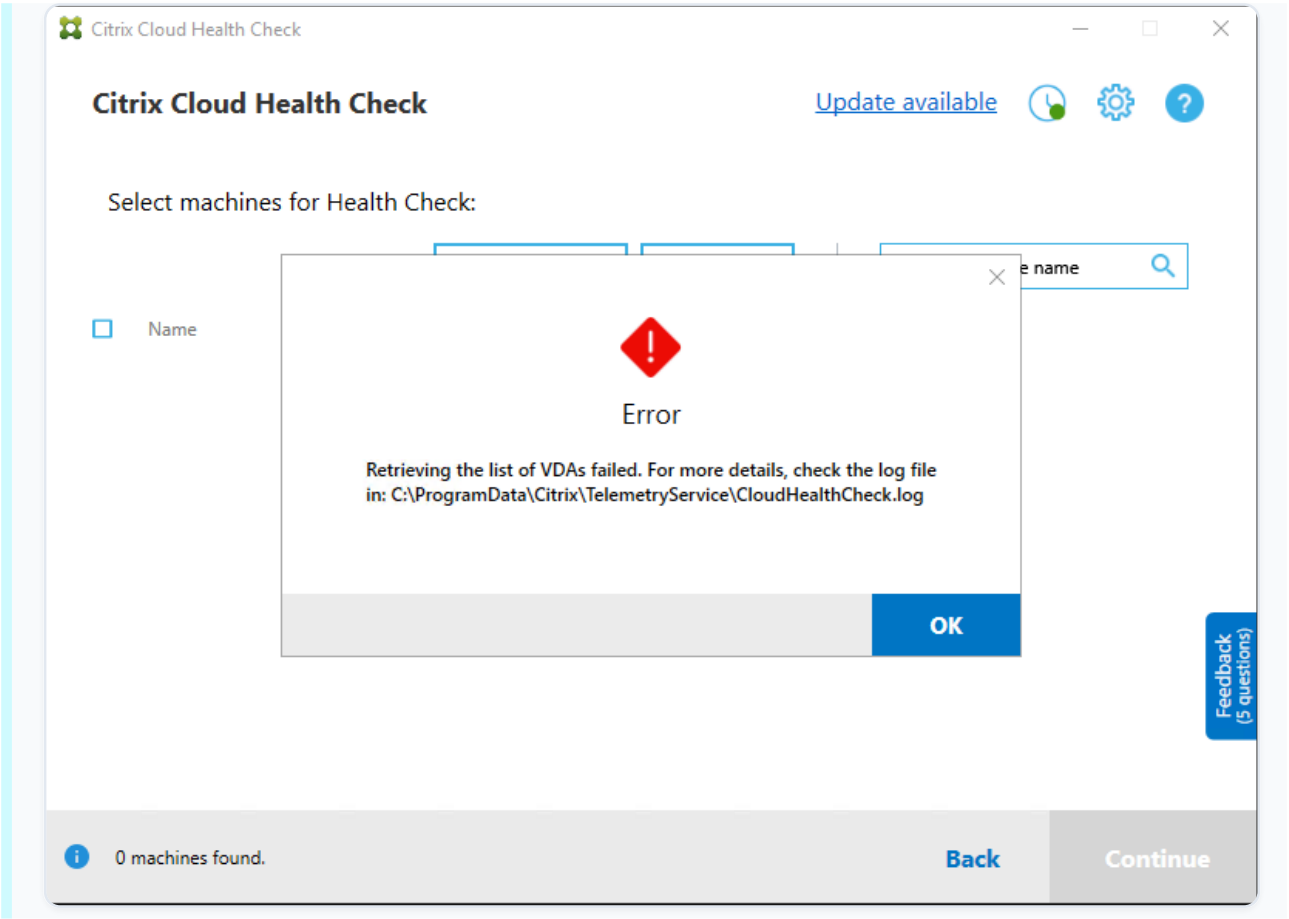
A lista de VDAs é exibida no Cloud Health Check. A lista também é salva em um arquivo local localizado em `\ProgramData\Citrix\TelemetryService\ChcDiscovery\ChcDiscoveredMachineList.json`.



Sua lista de máquinas carrega o cache local quando você abre o Cloud Health Check novamente. Se você fez alguma atualização em sua implantação, deve clicar em **Localizar máquina** para atualizar a lista de máquinas.

Nota:

- O Cloud Health Check encontra máquinas apenas na mesma floresta de domínio em que o Cloud Health Check está sendo executado.
- As sessões do Citrix Cloud expiram em uma hora. Após uma hora, você deve clicar em **Localizar máquina** novamente para obter a lista de VDAs mais recente.
- Uma mensagem de erro é exibida se a recuperação da lista de VDAs falhar. Você pode verificar os detalhes em `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.



Resultados da verificação de integridade

As verificações de integridade que geram relatórios contêm os seguintes elementos:

- Hora e data em que o relatório de resultados foi gerado
- FQDNs das máquinas que foram verificadas
- Condições verificadas nas máquinas de destino

Executando o Cloud Health Check na linha de comando

O Cloud Health Check pode ser executado na linha de comando para ajudar os clientes a realizar verificações de integridade. Para usar o Cloud Health Check na linha de comando, você deve ser um administrador na máquina em que o Cloud Health Check está sendo executado.

> **Nota:**
>
> Ao usar o Cloud Health Check na linha de comando, apenas uma máquina pode ser verificada por vez. Apenas uma instância de `CloudHealthCheck.exe` pode ser executada ao mesmo tempo na máquina de destino. Se você quiser verificar várias máquinas, as

> máquinas devem ser verificadas uma por uma, envolvendo os cmdlets em um loop em scripts de cmdlet/PowerShell. Qualquer instância de UI aberta do Cloud Health Check também deve ser fechada.

Argumentos de linha de comando

Os argumentos de linha de comando suportados são:

- `MachineFQDN` - Este argumento é **obrigatório**. Este é o nome de domínio totalmente qualificado da máquina de destino.
- `MachineType` - Este argumento é opcional. O valor do argumento pode ser o VDA do Windows (valor padrão) ou StoreFront.
- `ReportName` - Este argumento é opcional. O valor do argumento deve ser um nome de arquivo válido no Windows. O valor padrão é `HealthCheckReport`.
- `SkipAdminCheck` - Este argumento é opcional. Pode ser adicionado para ignorar as verificações que exigem permissões de administrador.
- `UpdateScripts` - Este argumento é opcional. Pode ser adicionado para atualizar os scripts de verificação do servidor CDN.
- `DisableCeip` - Este argumento é opcional. Se o CEIP estiver habilitado na UI, adicione-o para desabilitar o CEIP.
- `Help` - Mostra informações de ajuda sobre os parâmetros.

Exemplos:

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -ReportName checkreport
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -SkipAdminCheck
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -UpdateScripts
```

```
HealthCheckCLI.exe -MachineFQDN machine1.domain.local,machine2.domain.local,machine3.domain.local
```

```
HealthCheckCLI.exe -Help
```

> **Nota:**

> Os nomes dos parâmetros não diferenciam maiúsculas de minúsculas.

> Por padrão, a saída do console não é exibida na janela do console da linha de comando. Você pode exibir a saída manualmente anexando `|more` ao argumento.

Exemplo: `HealthCheckCLI.exe -MachineFQDN machine.domain.local|more`

O padrão da linha de comando requer permissões de administrador para ser executado. Adicione o parâmetro `-SkipAdminCheck` para ignorar a necessidade de permissões de administrador.

Códigos de saída

Os códigos de saída explicam o resultado das verificações do Cloud Health Check na linha de comando. Para obter o código de saída, você deve adicionar `start /wait` antes da linha de comando.

Exemplo: `start /wait HealthCheckCLI.exe -MachineFQDN machine.domain.local`

Os códigos de saída são:

- 0 - Normal, verificação concluída e aprovada.
- 1 - Falha, verificação concluída com problemas.
- 2 - Erro, verificação não concluída com erros.

Você também pode usar o argumento `echo %errorlevel%` para obter o código de saída do último comando executado.

Relatórios

O Cloud Health Check cria pastas com o nome da máquina em `HealthCheckDataFolder` para a máquina de destino. Um arquivo .html e um arquivo .json são criados na máquina onde o Cloud Health Check está instalado. Os relatórios de verificação de integridade estão localizados em `HealthCheckDataFolder` em `%ProgramData%\Citrix\TelemetryService\HealthCheck\Data`.

Os relatórios são criados apenas quando existem problemas na máquina de destino.

> **Observação:**

> Os arquivos de relatório são sobrescritos se o nome de relatório especificado já existir.

> Alertas e informações básicas são armazenados no relatório .json.

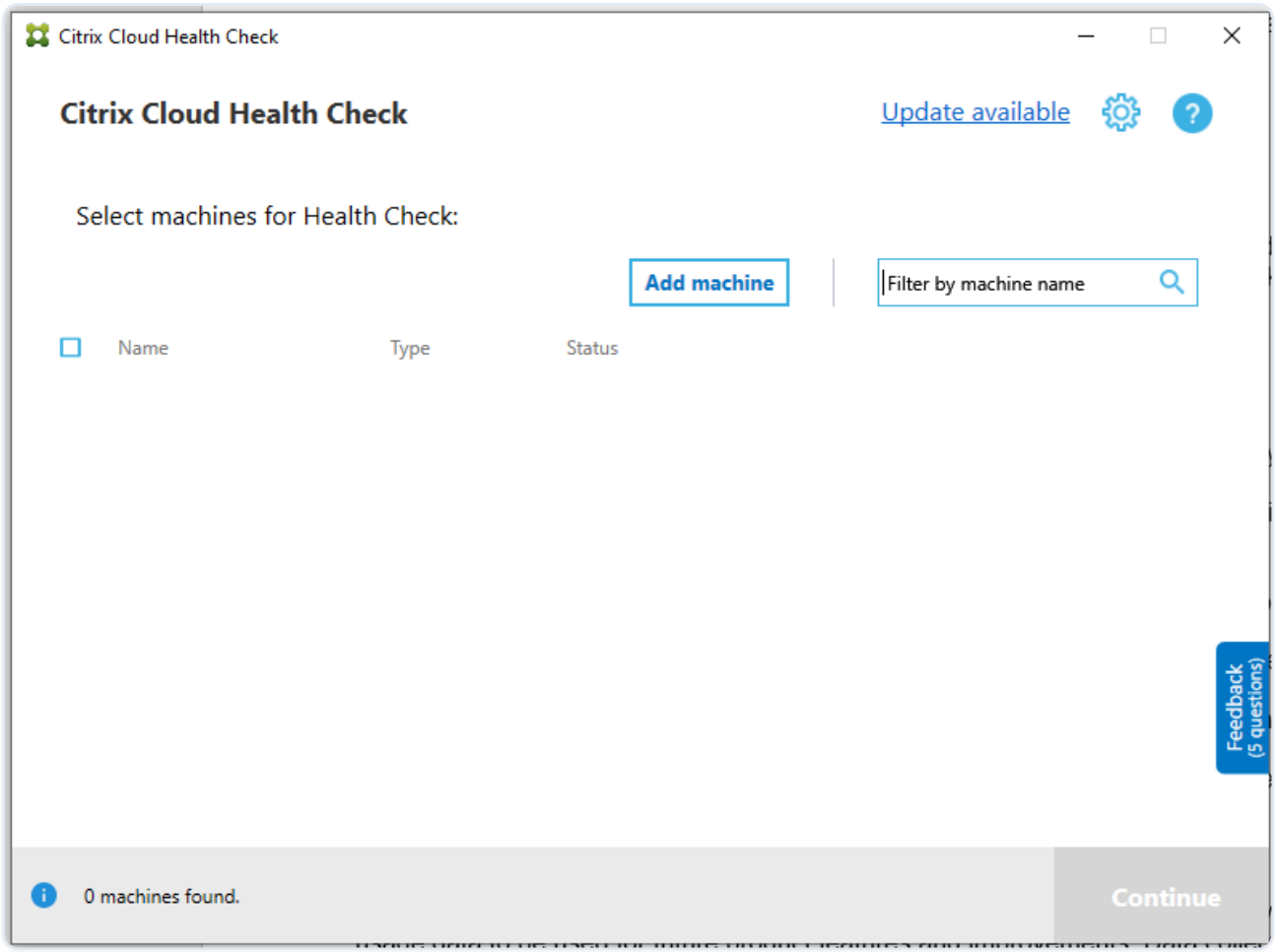


Os códigos de relatório são:

- **issueKey**: uma descrição em texto simples do problema.
- **issueUuid**: uma string de identificação exclusiva para o problema.
- **fixRecommendation**: a recomendação de correção para o problema.
- **severity**: indica se o problema deve ser corrigido. Um erro pode indicar que o componente (VDA ou StoreFront) funcionou mal, e um aviso indica que o componente pode funcionar, mas pode ter alguns problemas potenciais.
- **issueName**: o título do problema.
- **issueDescription**: uma descrição detalhada do problema.

Atualizando o Cloud Health Check

Se houver uma nova versão do Cloud Health Check disponível, um link de Atualização disponível será exibido no canto superior direito da janela do Cloud Health Check. Clique no link para ir para o Citrix Downloads e obter a nova versão.

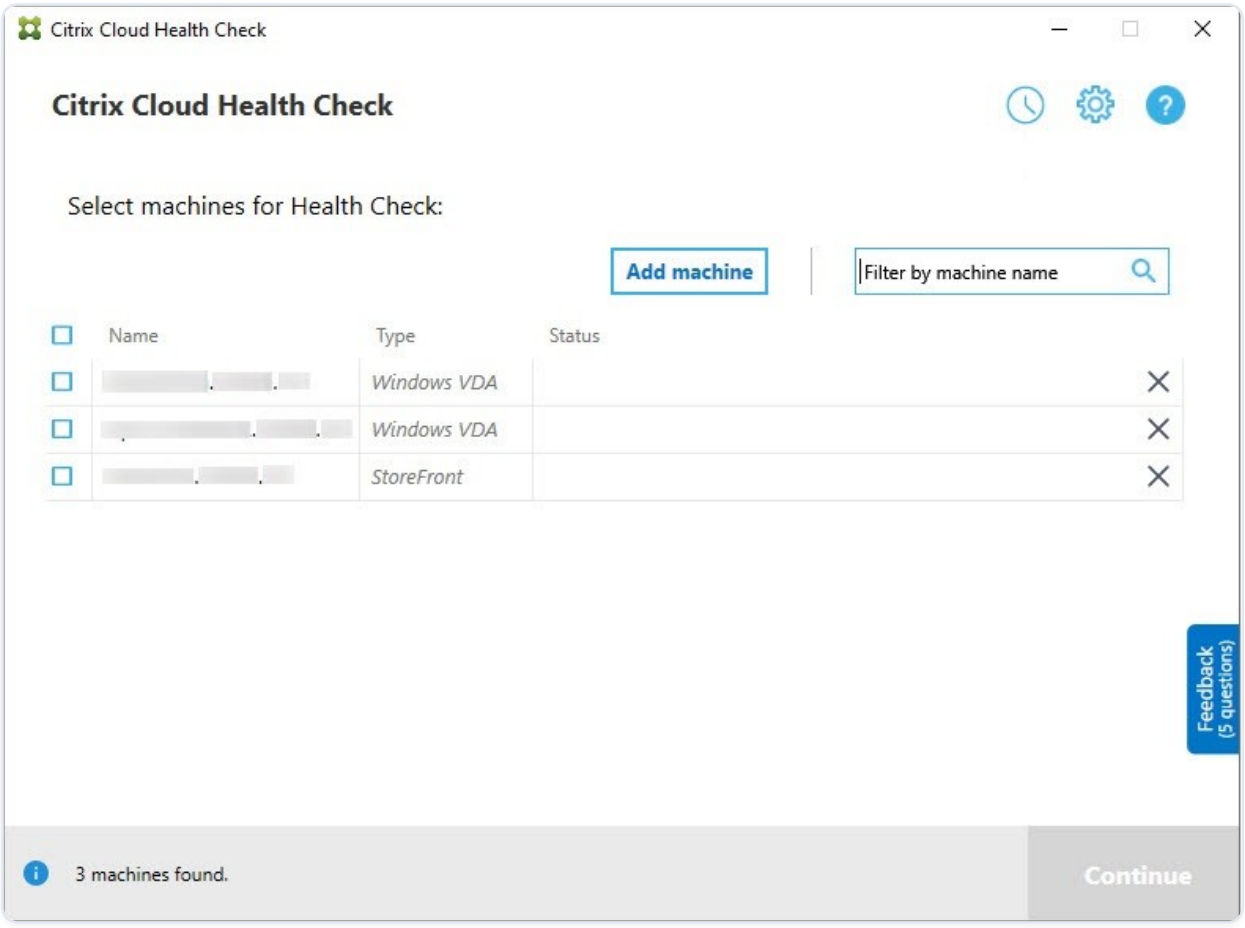


Agendador do Cloud Health Check

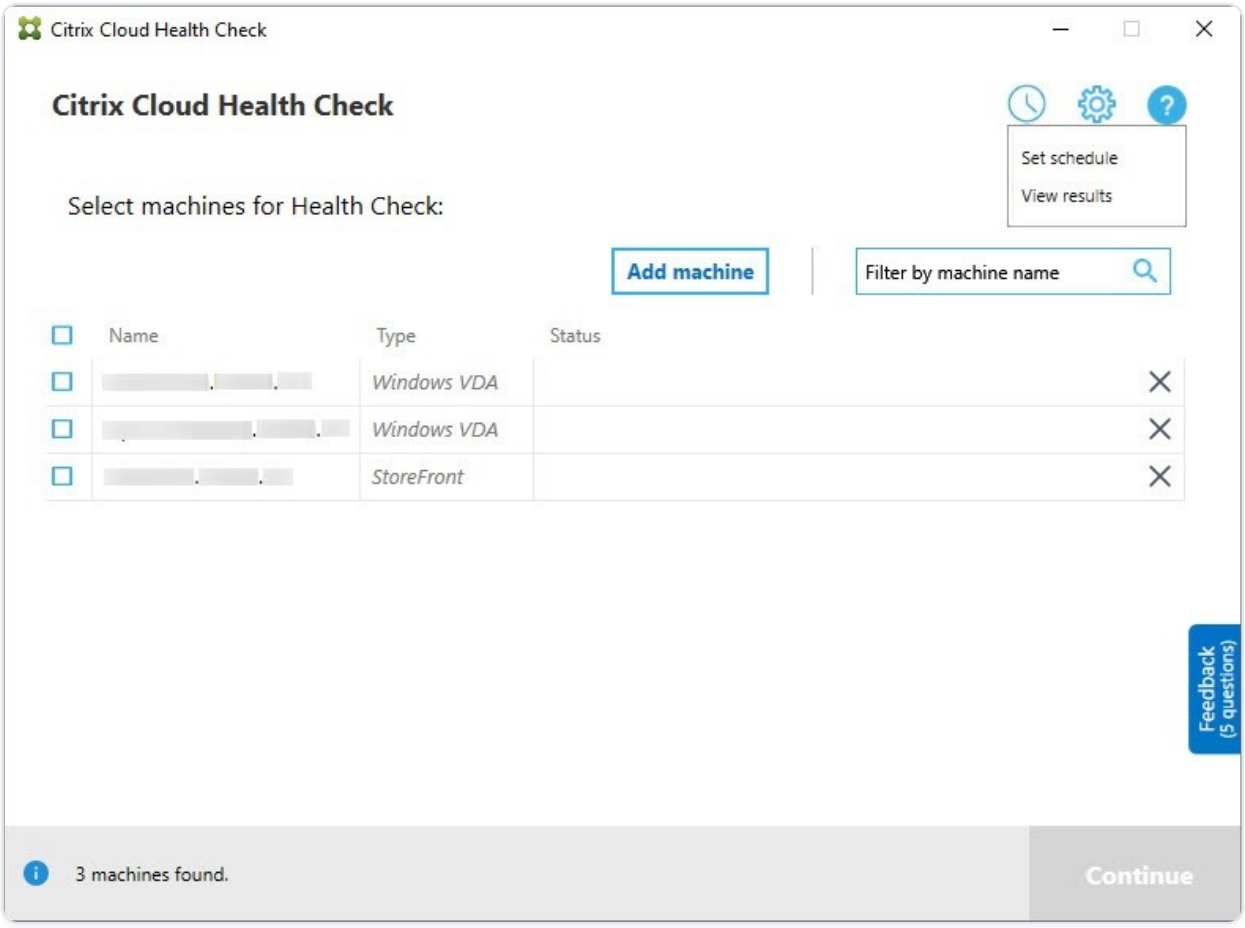
Use o agendador do Cloud Health Check para realizar verificações de integridade periódicas.

Configurar o agendamento

1. Clique em **Adicionar máquina** na janela principal do Cloud Health Check para adicionar as máquinas nas quais você deseja executar verificações periódicas.



2. Clique no ícone do relógio e, em seguida, clique em **Definir agendamento**.



3. Selecione um horário para o seu agendamento e, em seguida, clique em **Avançar**. A tarefa pode ser configurada para repetir selecionando a caixa de seleção **Repetir tarefa a cada**.
4. Escolha enviar os resultados para o Log de Eventos do Windows. A tarefa pode ser configurada para gravar os resultados no Log de Eventos do Windows.
5. Escolha acionar um script PowerShell personalizado após a conclusão da verificação agendada e, em seguida, clique em **Avançar**.

    - Clique em **Editar** para editar o conteúdo do script no Windows PowerShell ISE, se necessário.
    - Clique em **Localizar** para abrir o local do arquivo e usar um editor diferente para abrir o arquivo e editar o script.
    - Clique em **Redefinir** para redefinir o script para sua configuração original.

Nota:

- Você não pode alterar o nome e o caminho do script.
- Você pode implementar ações personalizadas usando o script ChcShceduledTrigger.ps1, como enviar um e-mail depois que o relatório de verificação agendada estiver pronto. Adicione o seguinte código ao final do script. Personalize o código para adicionar as contas de e-mail corretas e o endereço do servidor SMTP. Uma notificação por e-mail é enviada usando as credenciais da conta que executa a tarefa agendada.

```
#Sending email example code:

$body = "CreatedTime: $($report.CreatedTime)"

$body = $body + "`nStatusCode: $($report.StatusCode)"

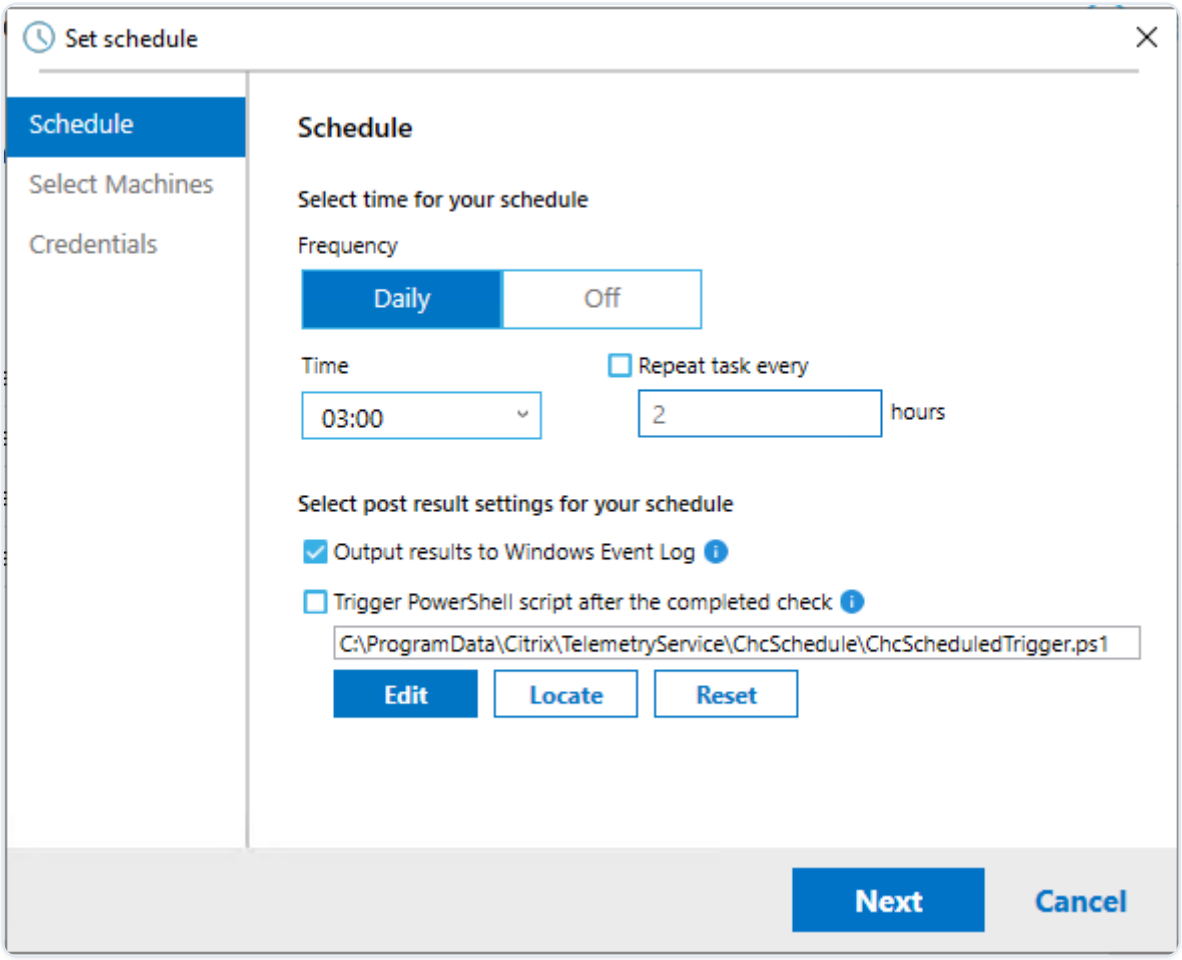
$body = $body + "`nMachineCount: $($report.MachineReports.Count)"

$from = "mock_email_accout"

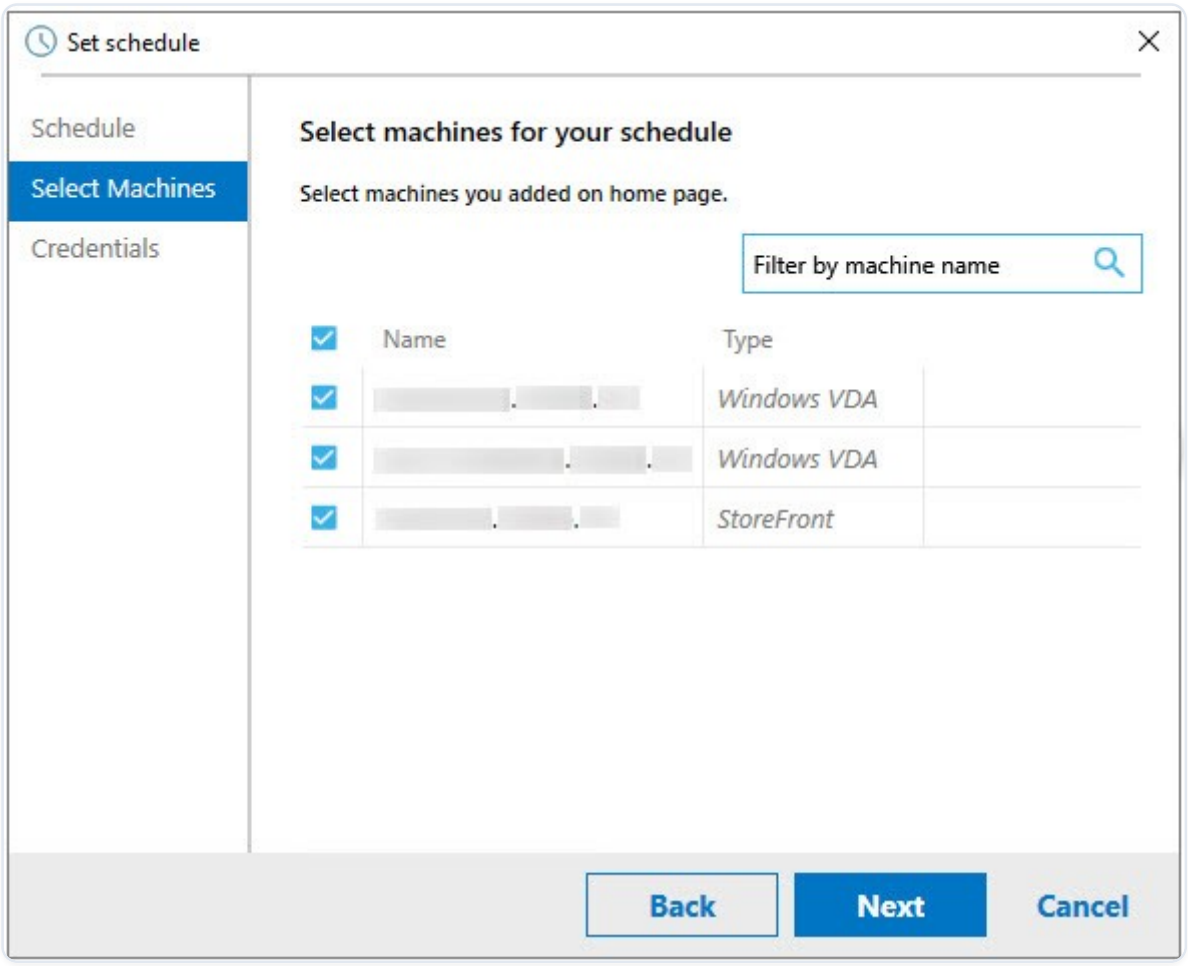
$to = "mock_email_accout"

$smtpServer = "mock_smtp_server"
```

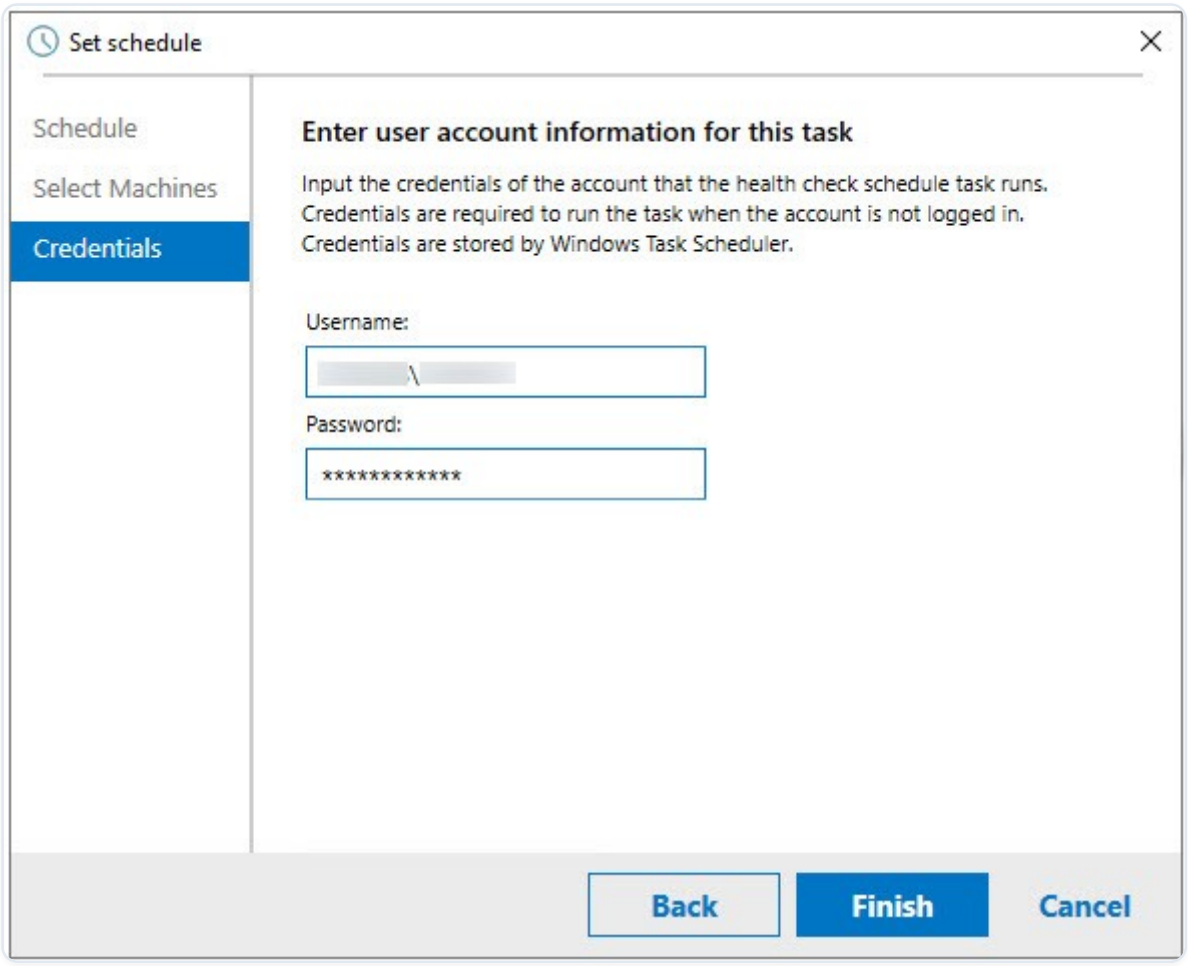
```
Send-MailMessage -Subject "Citrix Cloud Health Check Scheduler Report"
-Body $body -From $from -To $to -SmtpServer $smtpServer
```



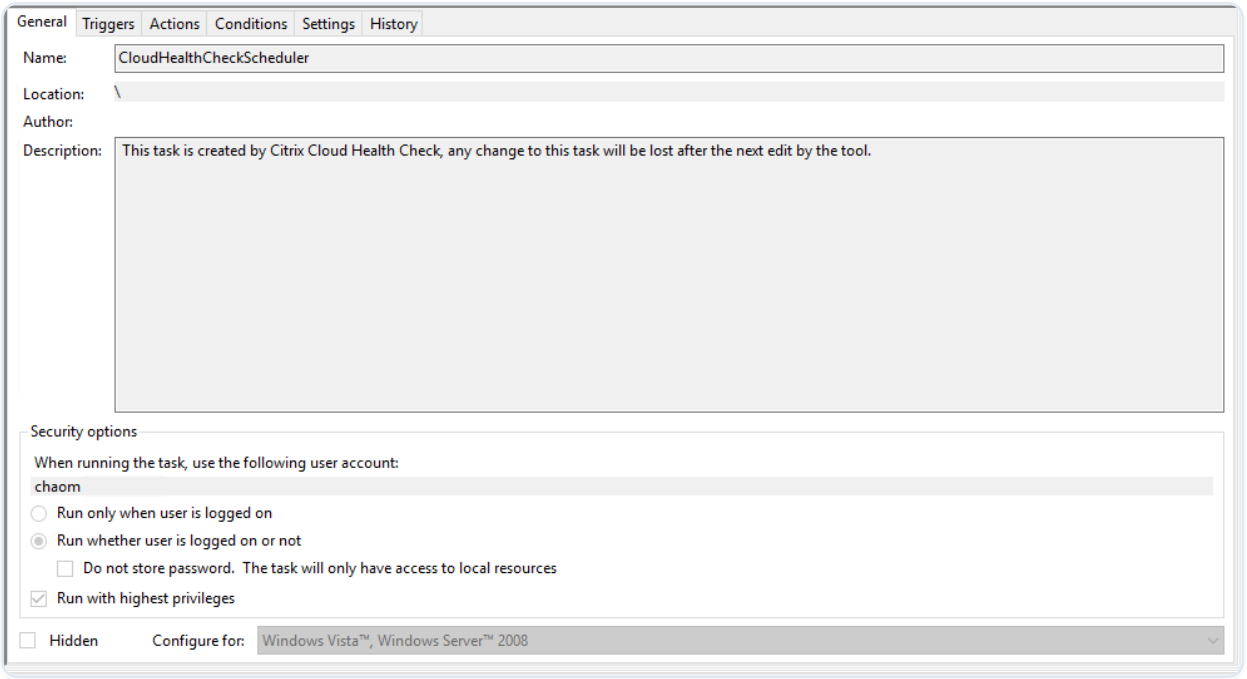
6. Selecione as máquinas para sua programação e clique em **Avançar**.



7. Insira as credenciais da conta em que a tarefa é executada e clique em **Concluir**.

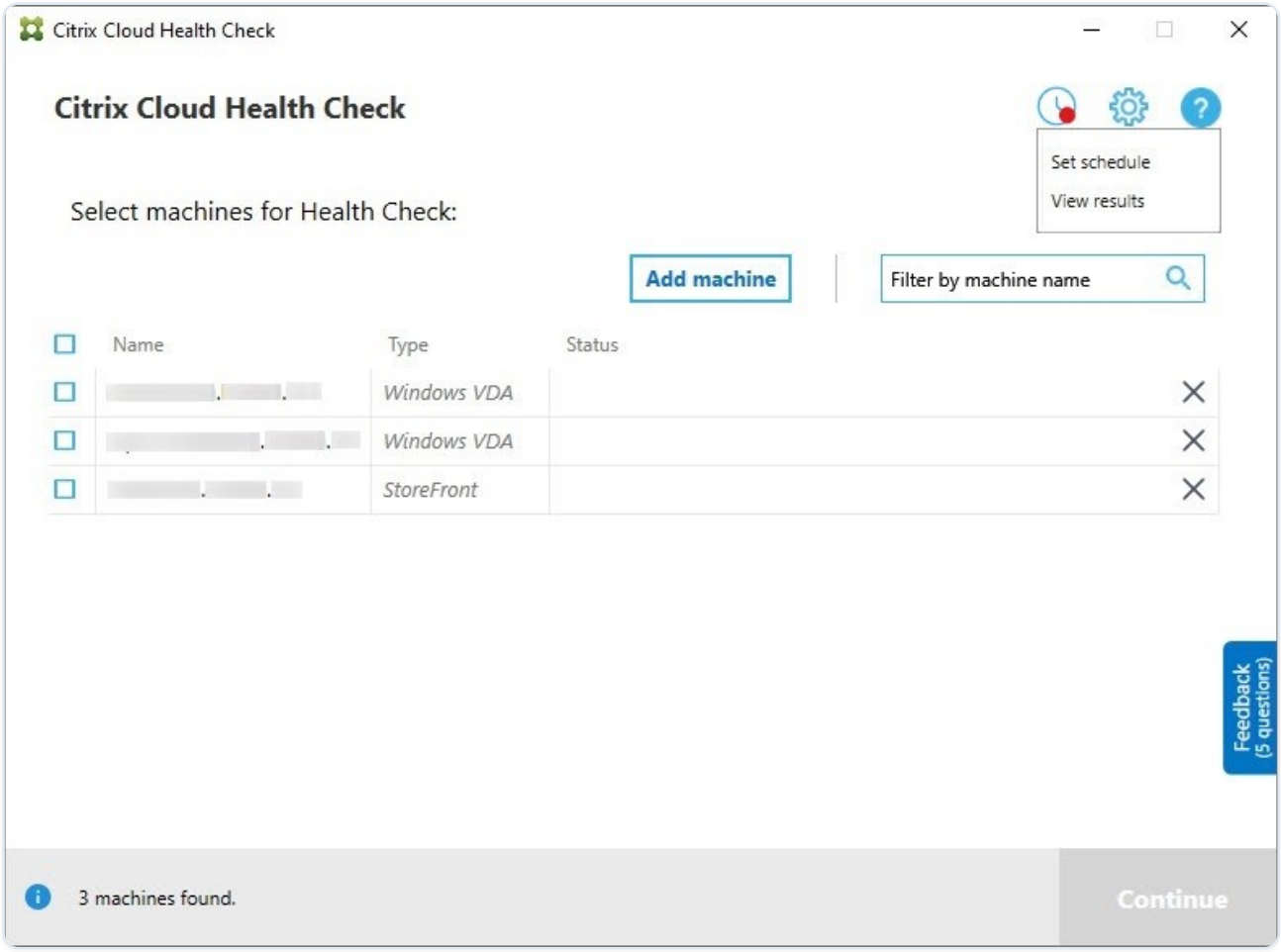


8. Uma tarefa CloudHealthCheckScheduler é criada no Agendador de Tarefas do Windows.

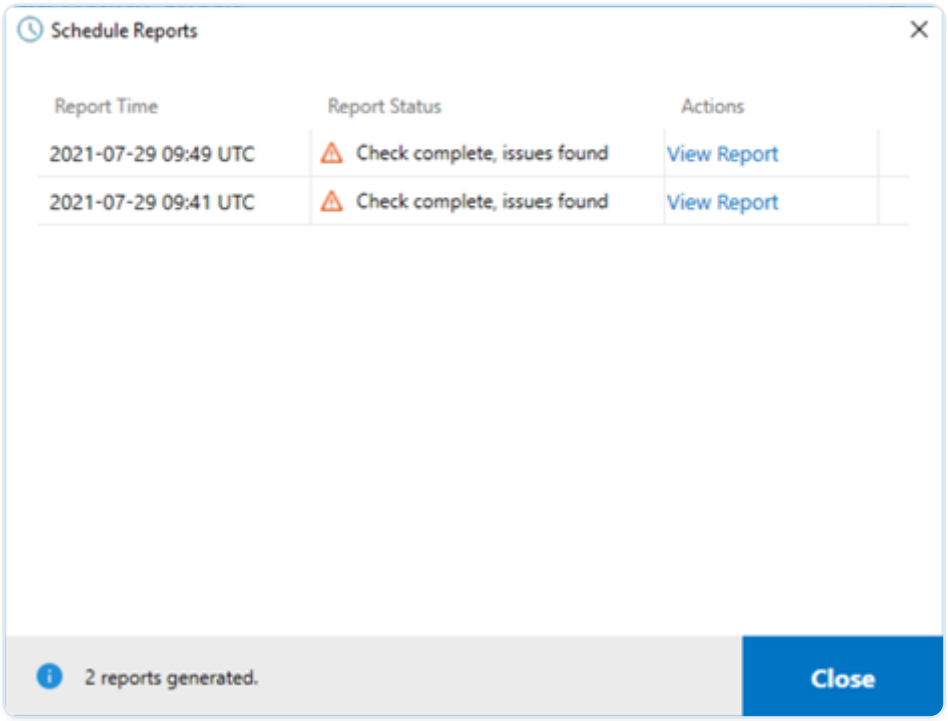


Exibir resultados da programação

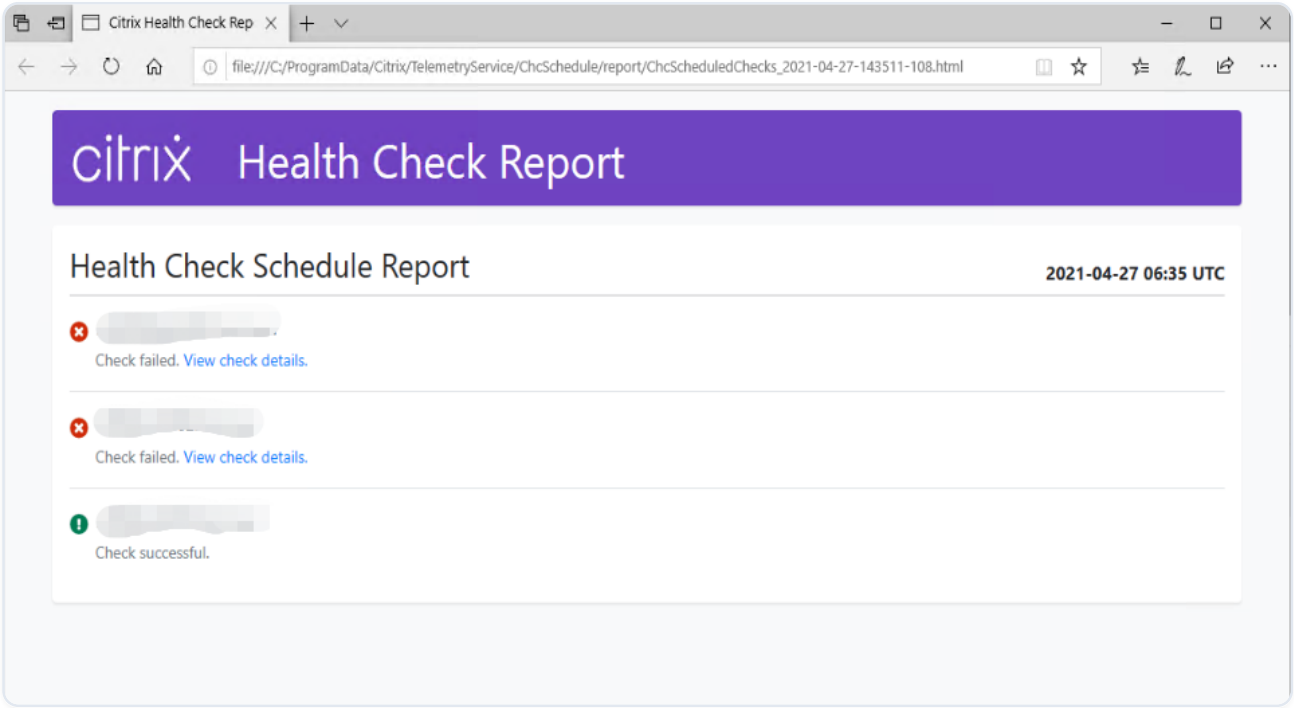
O ícone de relógio com um ponto vermelho indica que foram encontrados problemas na última verificação. Para exibir os resultados, clique no ícone de relógio e, em seguida, clique em **Exibir resultados**.



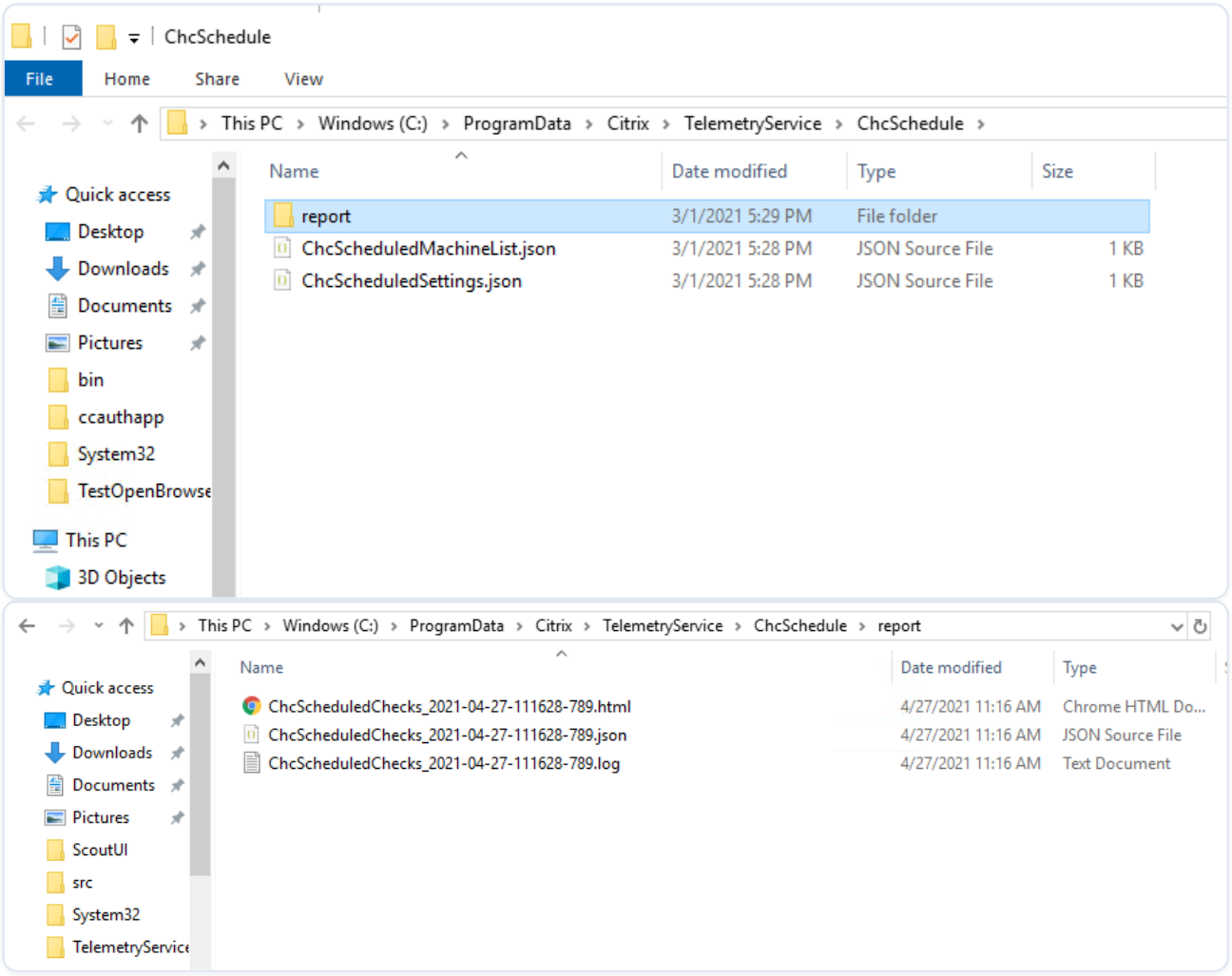
A página Relatórios Agendados mostra os resultados de todas as tarefas de verificação de integridade agendadas. Clique em **Exibir Relatório** para verificar o relatório de cada agendamento.



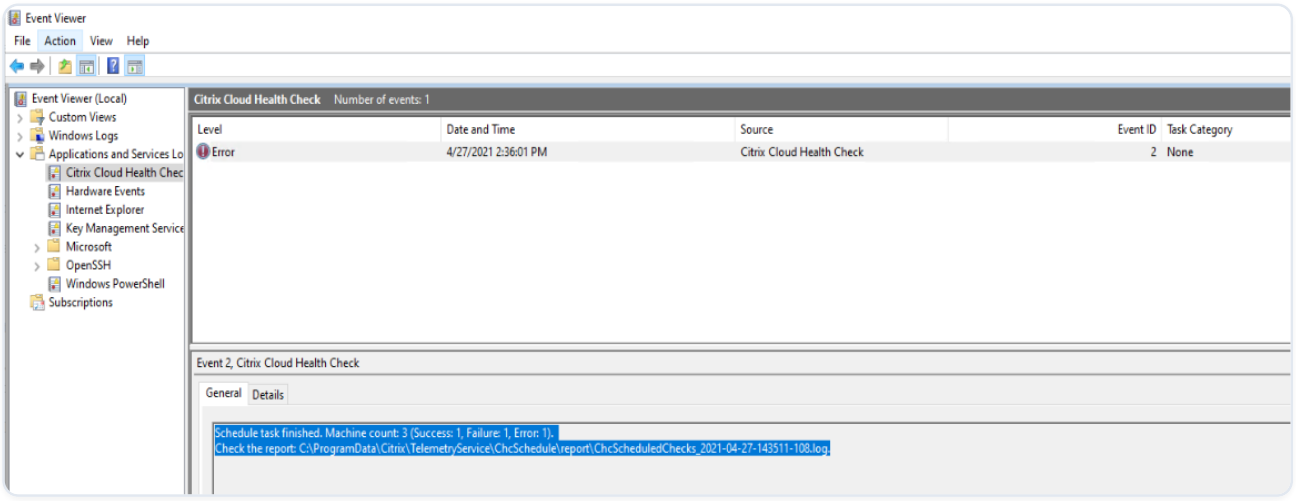
O relatório html lista o relatório geral para cada agendamento. Um exemplo do relatório está abaixo:



Todos os resultados da verificação de integridade são armazenados em uma pasta chamada ChcSchedule. O Cloud Health Check cria três arquivos durante cada execução da verificação. Até 500 logs de iteração são mantidos.

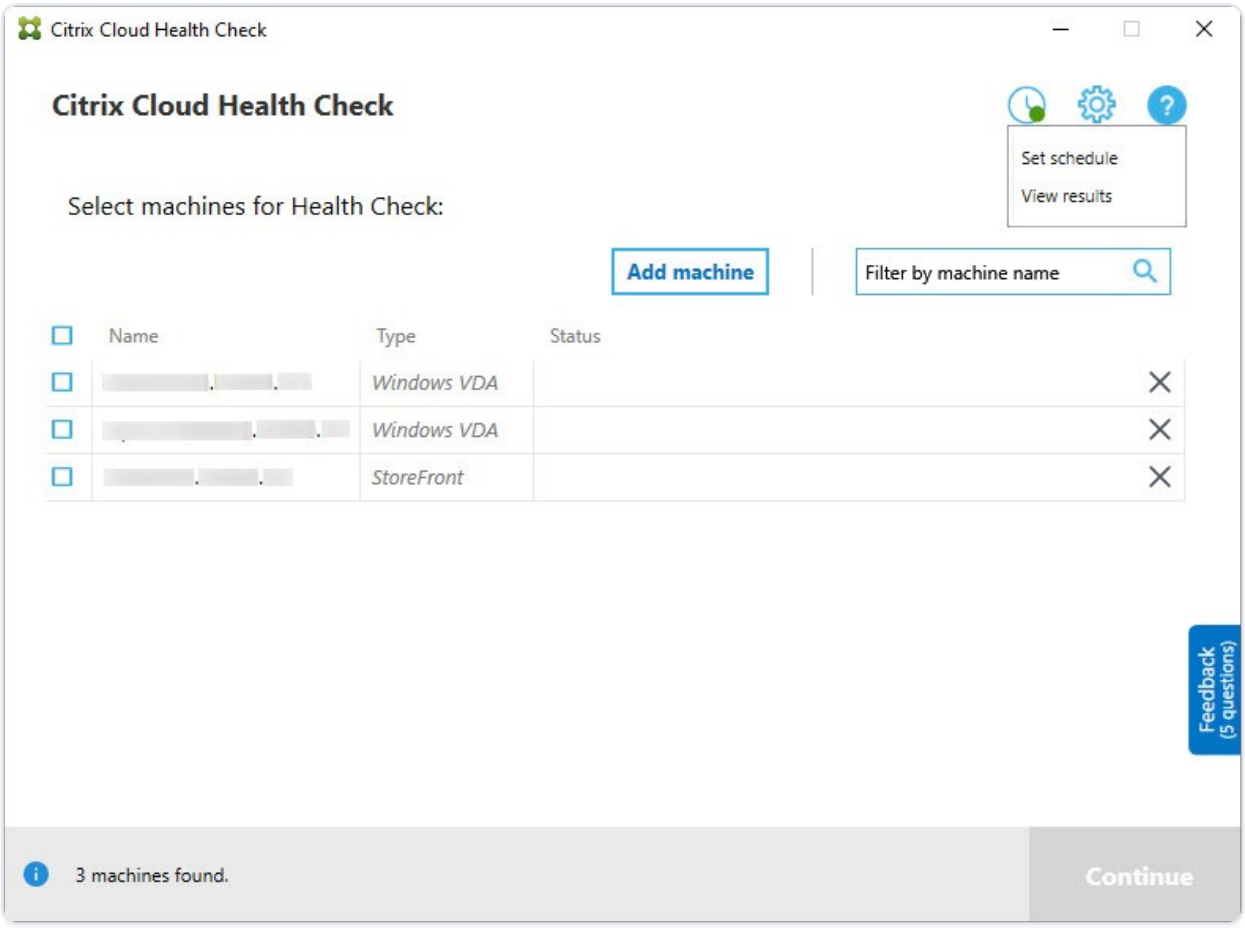


Se a caixa de seleção **Enviar resultados para o Log de Eventos do Windows** estiver selecionada, o resultado da verificação também é enviado para o Log de Eventos do Windows.

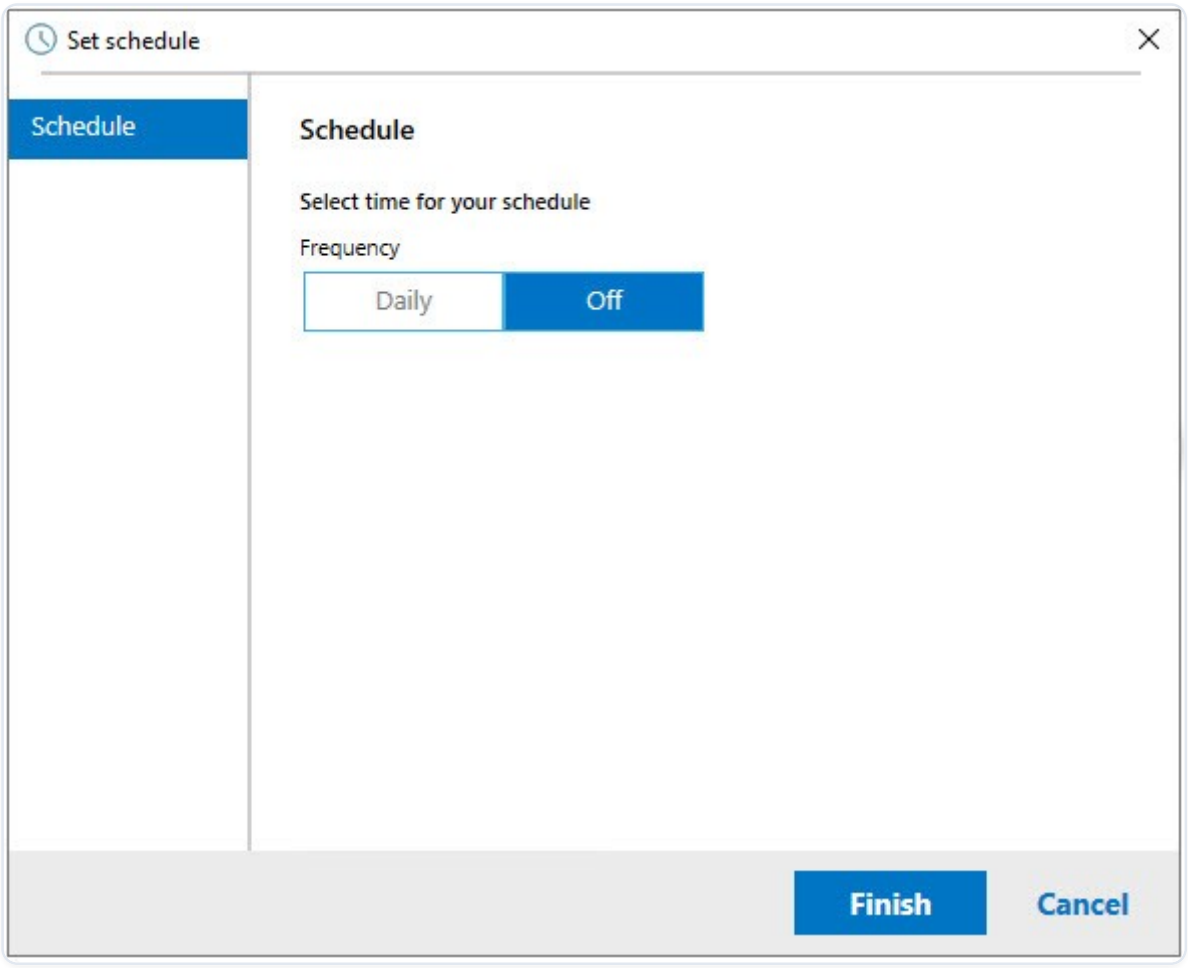


Desabilitar agendamentos

1. Clique no ícone do relógio e, em seguida, clique em **Definir agendamento**.



2. Clique em **Desativar** e, em seguida, clique em **Concluir** para desabilitar o agendador.



Mais informações

- Você deve adicionar ou importar VDAs para o Cloud Health Check primeiro. Para obter mais informações, consulte Importar Máquinas VDA.
- O agendador do Cloud Health Check pode agendar apenas uma tarefa por vez em uma máquina ingressada no domínio. Se você definir o agendamento várias vezes, apenas o mais recente terá efeito.

Testes de verificação

Antes que uma verificação de integridade seja iniciada, os testes de verificação são executados automaticamente para cada máquina selecionada. Esses testes garantem que os requisitos sejam atendidos para que uma verificação de integridade seja executada. Se um teste falhar para uma máquina, o Cloud Health Check exibirá uma mensagem com ações corretivas sugeridas.

- **O Cloud Health Check não consegue acessar esta máquina** - Certifique-se de que:
  - A máquina esteja ligada.
  - A conexão de rede esteja funcionando corretamente. (Isso pode incluir a verificação de que seu firewall está configurado corretamente.)

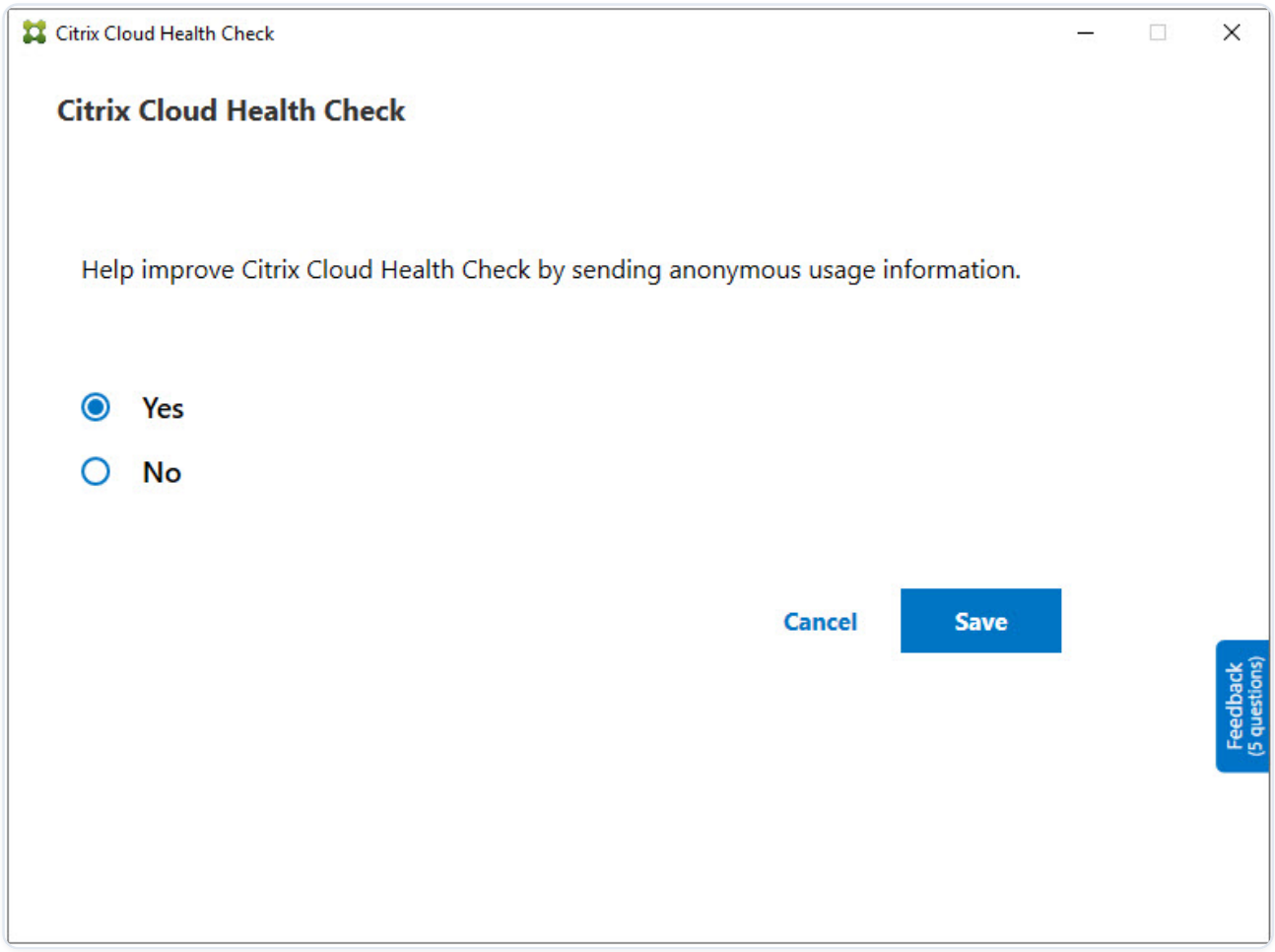
    - O compartilhamento de arquivos e impressoras esteja ativado. Consulte a documentação da Microsoft para obter instruções.

- **Habilitar PSRemoting e WinRM** - Você pode habilitar o PowerShell remoting e o WinRM executando o PowerShell como administrador e, em seguida, executando o cmdlet Enable-PSRemoting. Para obter detalhes, consulte a ajuda da Microsoft para o cmdlet.
- **O Cloud Health Check requer PowerShell 3.0 ou posterior** - Instale o PowerShell 3.0 ou posterior na máquina e, em seguida, habilite o PowerShell remoting.
- **O WMI não está sendo executado na máquina** - Certifique-se de que o acesso ao Windows Management Instrumentation (WMI) esteja habilitado.
- **Conexões WMI bloqueadas** - Habilite o WMI no serviço Firewall do Windows.

Coleta de dados de uso

Ao usar o Cloud Health Check, a Citrix usa o Google Analytics para coletar dados de uso anônimos a serem usados para futuros recursos e melhorias do produto. A coleta de dados é habilitada por padrão.

Para alterar a coleta e o upload de dados de uso, clique no ícone de engrenagem **Configurações** na interface do usuário do Cloud Health Check. Você pode então escolher se deseja enviar as informações selecionando **Sim** ou **Não** e, em seguida, clicando em **Salvar**.



Correção automática

A correção automática permite que o Cloud Health Check detecte e corrija automaticamente certos problemas alterando as configurações ou reiniciando os serviços.

A correção automática verifica os seguintes itens de registro do VDA, com as correções recomendadas:

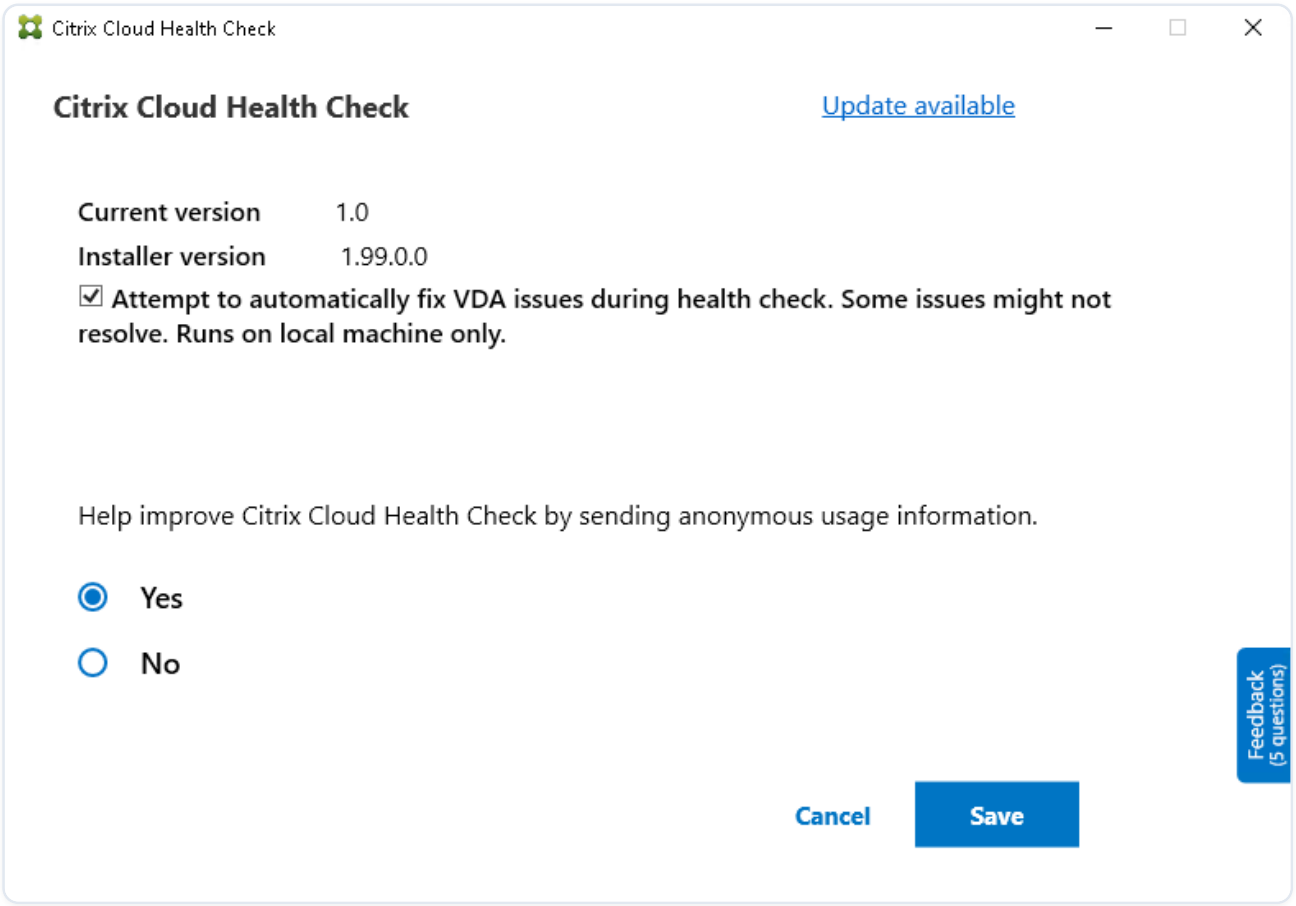
- Associação de domínio da máquina VDA
  - Correção: Testar o canal de segurança da conexão com um modelo de "reparo" para corrigir
- Status dos serviços VDA
  - Correção: Reiniciar o serviço BrokerAgent
- Comunicação com o Controller
  - Correção: Reiniciar o serviço BrokerAgent
- Sincronização de tempo com o Controller

- Correção: Executar o comando W32tm

Para inicializações de sessão, a correção automática verifica o seguinte item, com a correção recomendada:

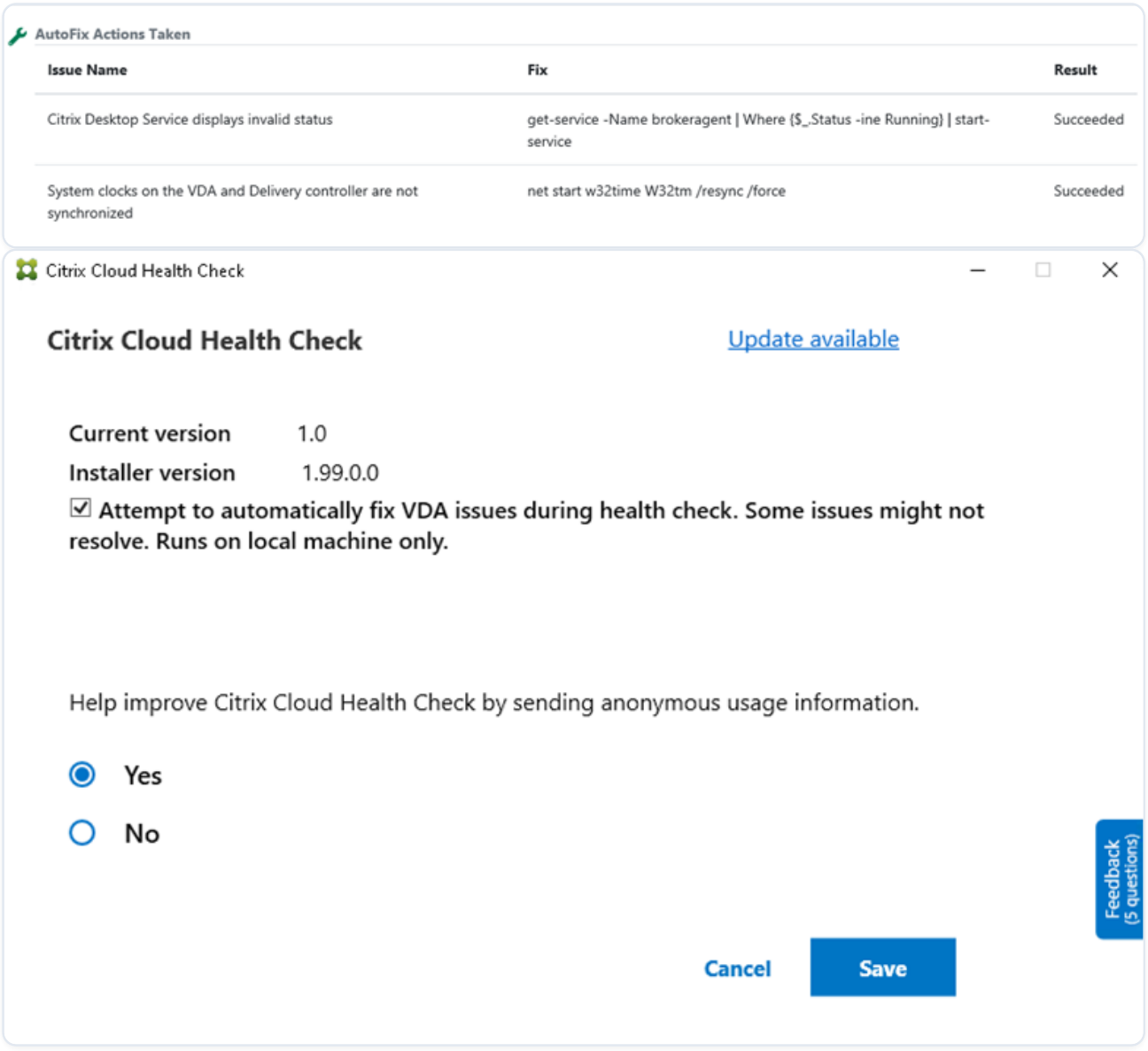
- Status do serviço de inicialização de sessão
  - Correção: Reiniciar o serviço BrokerAgent

Este recurso está habilitado por padrão. Para desativá-lo, clique no ícone de engrenagem no canto superior direito da janela principal do Cloud Health Check e desmarque **Tentar corrigir automaticamente problemas de VDA durante a verificação de integridade**.



Relatório de resultados

Após executar a correção automática, há uma seção no relatório de resultados da verificação para mostrar todos os detalhes:



Solução de problemas

Quando o Cloud Health Check falha ao ser executado ou ocorre qualquer exceção, verifique o log do Cloud Health Check em `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.

O log do Cloud Health Check para cada máquina de destino está em `C:\ProgramData\Citrix\TelemetryService\HealthCheck\Data\$TargetMachineFQDN\log.txt`.

Para habilitar o log de depuração:

Edite `C:\Program Files\Citrix\CloudHealthCheck\CloudHealthCheck.exe.config`, atualize `<add name="TraceLevelSwitch" value="3" /> to <add name="TraceLevelSwitch" value="4" />`, salve o arquivo e reabra o Cloud Health Check.

Comentários

Para deixar comentários sobre o Cloud Health Check, preencha a pesquisa da Citrix.

Registro de configuração

> **Nota:**
>
> Os registros de log de configuração aparecem apenas em inglês, independentemente do idioma selecionado para sua conta Citrix Cloud. As datas e horas associadas a esses registros estão no formato MM/DD/AA, expressas em Tempo Universal Coordenado (UTC).

> O registro de configuração é um recurso que captura as alterações de configuração de implantação e as atividades administrativas do Citrix Virtual Apps and Desktops™ e do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops) em um banco de dados de log no Citrix Cloud. Você pode usar o conteúdo registrado para:

- Diagnosticar e solucionar problemas após a realização de alterações de configuração. O log fornece um rastro de auditoria.
- Auxiliar no gerenciamento de mudanças e rastrear configurações.
- Relatar atividades administrativas.

Neste Citrix DaaS™, o registro de configuração está sempre ativado. Você não pode desativá-lo.

No Studio, você pode visualizar o conteúdo do log de configuração, filtrado por intervalos de datas ou por pesquisa de texto completo. Você também pode gerar um relatório CSV usando o PowerShell. A partir deste console, você não pode editar ou excluir o conteúdo do log. Você pode usar o SDK do PowerShell Remoto para agendar a exclusão periódica de dados do log.

Atualizar a retenção de logs de configuração do DaaS

Para manter o desempenho dos locatários do DaaS, a partir de 9 de setembro de 2024, a retenção de logs de configuração será definida para 180 dias.

Logs com mais de 180 dias em 9 de setembro de 2024 serão excluídos. À medida que continuamos a expandir nossos Limites do DaaS para um único locatário do DaaS, esta implementação garante o melhor desempenho e resiliência para nossos clientes.

Como uma boa prática, aconselhamos os clientes a ter um mecanismo de exportação trimestral. Isso pode ser feito via PowerShell, consulte Gerar relatórios. Também recomendamos que os clientes agendem a exclusão periódica de dados, consulte Agendar exclusão periódica de dados.

Permissões necessárias (consulte Administração delegada):

- Administradores Completos no Citrix Cloud™, além de Administradores de Nuvem do Citrix DaaS e Administradores Somente Leitura podem visualizar logs de configuração no Studio.
- Administradores Completos e Administradores de Nuvem também podem baixar um relatório CSV da atividade de registro, usando o PowerShell.

O que é registrado

As seguintes operações são registradas:

- Alterações de configuração e atividades administrativas iniciadas na seção **Gerenciar** e no nó **Monitorar**
- Scripts do PowerShell
- Solicitações da API REST

> **Nota:**

> Você não pode ver entradas de log para operações internas da plataforma Citrix Cloud, como configuração e gerenciamento de banco de dados.

> Exemplos de alterações de configuração registradas incluem trabalhar com (criar, editar, excluir, atribuir):

- Catálogos de máquinas
- Grupos de entrega (incluindo a alteração das configurações de gerenciamento de energia)
- Funções e escopos de administrador
- Recursos e conexões de host
- Políticas Citrix® via Studio

Exemplos de alterações administrativas registradas incluem:

- Gerenciamento de energia de uma máquina virtual ou de um desktop de usuário
- Gerenciar ou monitorar funções enviando uma mensagem para um usuário

As seguintes operações não são registradas. (Muitas delas não estão disponíveis para administradores de clientes.)

- Operações automáticas, como o ligamento de máquinas virtuais pelo gerenciamento de pool.
- Ações de política implementadas através do Console de Gerenciamento de Política de Grupo (GPMC). Use ferramentas da Microsoft para visualizar os logs dessas ações.
- Alterações feitas através do registro ou de outras fontes que não sejam Studio, Monitor ou PowerShell.

Visualizar conteúdo do log de configuração

Para visualizar o conteúdo do log de configuração, siga estas etapas:

1. Faça login em Citrix Cloud.
2. No bloco **DaaS**, clique em **Gerenciar**.
3. Selecione **Registro** no painel esquerdo e clique na guia **Eventos**.

Por padrão, os logs de eventos são listados pelos nomes dos administradores. Você pode executar as seguintes tarefas conforme necessário:

- **Classificar a exibição.** Classifique a exibição clicando em um cabeçalho de coluna.
- **Filtrar logs.** Refine a exibição definindo filtros, como:
  - Intervalos de dias ou períodos personalizados.
  - Nomes de Tarefas Principais completos ou parciais.
  - Detalhes de operações de baixo nível, como nome da máquina e nome VDI. Para pesquisar em detalhes de baixo nível, selecione **Estender escopo de pesquisa para incluir detalhes** antes de inserir seu termo de pesquisa.

    > **Nota:**
    >
    > - Habilitar esta opção pode aumentar o tempo de pesquisa porque o sistema pesquisa um conjunto mais amplo de entradas de log.
    > - A seleção é salva apenas para a sessão atual do Web Studio. Ao sair ou iniciar uma nova sessão, selecione a opção novamente se desejar incluir detalhes de operações de baixo nível na pesquisa.

- **Exportar logs.** Exporte logs selecionados ou todos os logs para um arquivo CSV para arquivamento ou análise posterior.
- **Personalizar colunas.** Adapte a exibição às suas necessidades adicionando colunas não padrão, como IP do Cliente e Rótulos.
- **Gerenciar rótulos.** Adicione, edite e remova rótulos para logs de eventos para aprimorar a organização e o rastreamento de logs.

Características de exibição:

- Operações de alto nível criadas durante o gerenciamento e monitoramento são listadas no painel superior central. Uma operação de alto nível resulta em um ou mais serviços e chamadas de SDK do PowerShell, que são operações de baixo nível. Ao selecionar uma operação de alto nível no painel superior central, o painel inferior exibe as operações de baixo nível.
- Se você criar uma operação de baixo nível no PowerShell sem especificar uma operação de alto nível pai, o registro de configuração criará uma operação de alto nível substituta.
- Se uma operação falhar antes da conclusão, a operação de log pode não ser concluída no banco de dados. Por exemplo, um registro de início não tem um registro de parada correspondente. Nesses casos, o log indica que há informações ausentes. Ao exibir logs com base em intervalos de tempo, logs incompletos são mostrados se os dados nos logs corresponderem aos critérios. Por exemplo, se você solicitar logs dos últimos cinco dias, e um log com um horário de início nos últimos cinco dias não tiver um horário de término, ele será incluído.
- Lembre-se: Você não pode ver entradas de log para operações internas da plataforma Citrix Cloud, como configuração e gerenciamento de banco de dados.

Visualizar tarefas relacionadas a operações de catálogo de máquinas

Para visualizar tarefas relacionadas a operações de catálogo de máquinas, navegar para **Logging > Tasks**. A guia **Tasks** exibe apenas tarefas relacionadas a catálogos criados através do Machine Creation Services™ (MCS) ou Provisioning Services (PVS). Especificamente, aparecem as tarefas associadas às seguintes operações de catálogo de máquinas:

- Criar catálogos
- Clonar catálogos
- Adicionar máquinas
- Remover máquinas

- Atualizar um catálogo (atualizar imagens ou máquinas)
- Reverter atualizações de máquina

> **Dica:**

> A guia **Tarefas** exibe apenas tarefas relacionadas a alterações de esquema de provisionamento (criação ou modificação de um esquema de provisionamento).

> Uma tarefa pode estar no seguinte estado:

- Concluída
- Não iniciada
- Em execução
- Cancelada
- Falhou
- Desconhecido

Para cancelar uma tarefa em execução, selecione a tarefa e clique em **Cancelar**. O cancelamento leva algum tempo para ser concluído.

Exemplos de tarefas registradas incluem:

- Atualização de imagem concluída para um determinado catálogo
- Erro ao atualizar a imagem para um determinado catálogo
- Atualização de imagem cancelada para um determinado catálogo
- Provisionando VMs para um determinado catálogo
- Removendo VMs de um determinado catálogo
- Catálogo criado

Por padrão, a exibição no painel central lista as tarefas registradas cronologicamente (entradas mais recentes primeiro), separadas por data. Você pode classificar a exibição pelo cabeçalho da coluna. Para limpar as tarefas concluídas, clique em **Limpar Tarefas Concluídas** na guia **Tarefas**. Para escolher quais colunas aparecerão na exibição, selecione o ícone **Colunas a Exibir** no canto superior direito da tabela.

Exibir logs da API

Para exibir os logs da API REST, navegar para **Logging > APIs**. A guia **APIs** exibe as solicitações da API REST feitas durante um determinado período.

Esteja ciente das seguintes considerações:

- Os logs da API REST são limpos depois que você sai do console. (Eles também são limpos se você atualizar a janela do navegador.)
- Quaisquer operações no console que resultem em chamadas de API têm suas solicitações de API correspondentes exibidas na guia **APIs**.
- A exibição lista as solicitações da API cronologicamente (entradas mais recentes primeiro), separadas por data. O número máximo de solicitações da API na exibição é 1.000.

Visualizar logs do PowerShell

Para visualizar os comandos do PowerShell correspondentes às ações da interface do usuário que você realizou durante o dia, navegar até a guia **Logging > PowerShell**.

Associar metadados a logs de configuração

Você pode anexar metadados aos logs de configuração associando um par `name-value` chamado `MetadataMap` aos registros de log.

> **Nota:**
>
> - Você só pode anexar metadados a objetos de operação de alto nível.
> - Os metadados são associados aos registros existentes no momento da execução.

Definir os metadados

Execute o comando PowerShell `Set-LogHighLevelOperationMetadata` para associar um registro de log ao `MetadataMap`. `Set-LogHighLevelOperationMetadata` aceita os seguintes parâmetros:

- **Id**: ID da operação de alto nível.
- **InputObject**: As operações de alto nível às quais você adiciona os metadados. Esta é uma alternativa ao parâmetro `Id` onde um objeto de operação de alto nível ou uma lista de objetos é passado para o comando PowerShell.

- **Name**: Nome da propriedade dos metadados a serem adicionados. A propriedade deve ser única para a operação de alto nível especificada. A propriedade não pode conter nenhum dos seguintes caracteres: `()\/;:#.*?=<>|[]"'`
- **Value**: Valor para a propriedade.
- **Map**: Dicionário de pares (nome, valor) para as propriedades. Esta é uma alternativa para definir os metadados usando os parâmetros `-Name` e `-Value`.

Por exemplo, para anexar os metadados a todos os registros de log de alto nível com Id 40, execute o seguinte comando PowerShell:

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

Para anexar os metadados ao registro de alto nível com o usuário `abc@example.com`, execute o seguinte comando PowerShell:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperationMetadata -Name C -Value D
```

Recuperar usando os metadados

Execute os seguintes comandos PowerShell para usar os metadados associados para recuperar os registros de log:

- Pesquisar por chave e valor:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Pesquisar por valor e qualquer chave:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Pesquisar por chave e qualquer valor:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

Remover os metadados

Execute o comando PowerShell `Remove-LogHighLevelOperationMetadata` para remover os metadados associados. `Remove-LogHighLevelOperationMetadata` aceita os seguintes parâmetros:

- **Id**:ID da operação de alto nível.

- **InputObject**:As operações de alto nível às quais você adiciona os metadados. Esta é uma alternativa ao parâmetro `Id`` onde um objeto de operação de alto nível ou lista de objetos é passado para o comando PowerShell.
- **Nome**: Nome da propriedade dos metadados a serem removidos. Defina como $null para remover todos os metadados do objeto especificado.
- **Mapa**: Dicionário de pares (nome, valor) para as propriedades. Pode ser uma hashtable (criada com @{"name1" = "val1"; "name2" = "val2"}) ou um dicionário de strings (criado com new-object "System.Collections.Generic.Dictionary"). As propriedades cujos nomes correspondem às chaves no mapa são removidas.

Gerar relatórios

Para gerar um relatório CSV ou HTML contendo dados de log de configuração, use os cmdlets do PowerShell para o Serviço ConfigLogging no SDK do PowerShell Remoto do Citrix Virtual Apps and Desktops. Para obter detalhes, consulte:

- `Export-LogReportCsv`
- `Export-LogReportHtml`

Agendar exclusão periódica de dados

Use o SDK do PowerShell Remoto para especificar por quanto tempo os dados são retidos no banco de dados de log de configuração. (Este recurso não está disponível no Studio.) No Citrix DaaS, você deve ter acesso total.

No cmdlet `Set-LogSite`, o parâmetro `-LoggingDBPurgeDurationDays` especifica por quantos dias os dados são retidos no banco de dados de log de configuração antes de serem excluídos automaticamente.

- Por padrão, o valor deste parâmetro é 0. Um valor zero significa que os dados no banco de dados de log de configuração nunca são excluídos automaticamente.
- Quando você define um valor diferente de zero, o banco de dados é verificado uma vez a cada 120 minutos. Os dados mais antigos que o período de retenção são excluídos.

Use `Get-LogSite` para visualizar o valor atual do parâmetro.

Diferenças em relação ao Citrix Virtual Apps and Desktops local

Se você está familiarizado com o log de configuração no produto Virtual Apps and Desktops local, a versão do Citrix Cloud apresenta várias diferenças. No Citrix Cloud:

- O log de configuração está sempre ativado. Você não pode desativá-lo. O log obrigatório não está disponível.
- Você não pode alterar o local do banco de dados de log de configuração, porque o banco de dados é gerenciado na plataforma Citrix Cloud.
- As exibições de log de configuração não incluem operações e atividades que são realizadas na plataforma Citrix Cloud.
- O PowerShell é sua única opção para criar um relatório CSV ou HTML de operações registradas. No produto local, os relatórios podem ser gerados a partir do Citrix Studio ou do PowerShell.
- Você não pode excluir o conteúdo do log de configuração.

Administração delegada

Visão geral

Com a administração delegada no Citrix Cloud™, você pode configurar as permissões de acesso que todos os seus administradores precisam, de acordo com sua função em sua organização.

Por padrão, os administradores têm acesso total. Essa configuração permite o acesso a todas as funções de administração e gerenciamento de clientes disponíveis no Citrix Cloud, além de todos os serviços assinados. Para personalizar o acesso de um administrador:

- Configure o acesso personalizado para as permissões de gerenciamento geral de um administrador no Citrix Cloud.
- Configure o acesso personalizado para serviços assinados. No Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™), você pode configurar o acesso personalizado ao convidar um novo administrador. Você pode alterar o acesso de um administrador posteriormente.

Para obter informações sobre como exibir a lista de administradores e definir permissões de acesso, consulte Gerenciar acesso de administrador ao Citrix Cloud.

Este artigo descreve como configurar o acesso personalizado no Citrix DaaS.

Administradores, funções e escopos

A administração delegada usa três conceitos para acesso personalizado: administradores, funções e escopos.

- **Administradores:** Um administrador representa uma pessoa identificada por seu login no Citrix Cloud, que geralmente é um endereço de e-mail. Cada administrador está associado a um ou mais pares de função e escopo.
- **Funções:** Uma função representa uma função de trabalho e tem permissões associadas a ela. Essas permissões permitem certas tarefas que são exclusivas do Citrix DaaS. Por exemplo, a função de Administrador de Grupo de Entrega tem permissão para criar um grupo de entrega e remover um desktop de um grupo de entrega, além de outras permissões associadas. Um administrador pode ter várias funções. Um administrador pode ser um Administrador de Grupo de Entrega e um Administrador de Catálogo de Máquinas.

  O Citrix DaaS oferece várias funções de acesso personalizado integradas. Você não pode alterar as permissões dentro dessas funções integradas, nem excluí-las.

  Você pode criar suas próprias funções de acesso personalizado para atender aos requisitos da sua organização e delegar permissões com mais detalhes. Use funções personalizadas para alocar permissões na granularidade de uma ação ou tarefa. Você pode excluir uma função personalizada somente se ela não estiver atribuída a um administrador.

  Você pode alterar quais funções um administrador possui.

  Uma função é sempre emparelhada com um escopo.
- **Escopos:** Um escopo representa uma coleção de objetos. Os escopos são usados para agrupar objetos de uma forma que seja relevante para sua organização. Os objetos podem estar em mais de um escopo.

  Existe um escopo integrado: Todos, que contém todos os objetos. Os administradores do Citrix Cloud e do Help Desk são sempre emparelhados com o escopo Todos. Esse escopo não pode ser alterado para esses administradores.

  Quando você convida (adiciona) um administrador para este serviço, uma função é sempre emparelhada com um escopo (por padrão, o escopo Todos).

  Você cria e exclui escopos usando o Studio. Você atribui pares de função/escopo no console do Citrix Cloud.

  Um escopo não é exibido para administradores de acesso total. Por definição, esses administradores podem acessar todos os objetos de serviços inscritos e do Citrix Cloud gerenciados pelo cliente.

Funções e escopos integrados

O Citrix DaaS possui as seguintes funções integradas.

- **Administrador de Nuvem:** Pode executar todas as tarefas e operações para gerenciar o DaaS.

  Pode ver os consoles **Gerenciar** e **Monitorar** no Studio. Esta função é sempre combinada com o escopo Todos. Você não pode alterar o escopo.

  Não se confunda com o nome desta função. Um Administrador de Nuvem de acesso personalizado não pode executar tarefas de nível Citrix Cloud (as tarefas do Citrix Cloud exigem acesso total).
- **Administrador Somente Leitura:** Pode ver todos os objetos nos escopos especificados (além das informações globais), mas não pode alterar nada. Por exemplo, um Administrador Somente Leitura com um escopo de Londres pode ver todos os objetos globais e quaisquer objetos no escopo de Londres (por exemplo, Grupos de Entrega de Londres). No entanto, esse administrador não pode ver objetos no escopo de Nova York (assumindo que os escopos de Londres e Nova York não se sobreponham).

  Pode ver os consoles **Gerenciar** e **Monitorar** no Studio.
- **Administrador de Help Desk:** Pode visualizar grupos de entrega e gerenciar as sessões e máquinas associadas a esses grupos. Pode ver o catálogo de máquinas e as informações do host para os grupos de entrega que estão sendo monitorados. Também pode executar operações de gerenciamento de sessão e gerenciamento de energia de máquinas para as máquinas nesses grupos de entrega.

  Pode ver o console **Monitorar** no Studio. Não pode ver o console **Gerenciar**. Esta função é sempre combinada com o escopo Todos. Você não pode alterar o escopo.
- **Administrador de Catálogo de Máquinas:** Pode criar e gerenciar catálogos de máquinas e provisionar as máquinas neles. Pode gerenciar imagens base e instalar software, mas não pode atribuir aplicativos ou desktops a usuários.

  Pode ver os consoles **Gerenciar** e **Monitorar** no Studio. Você pode alterar o escopo.
- **Administrador de Grupo de Entrega:** Pode entregar aplicativos, desktops e máquinas. Também pode gerenciar as sessões associadas. Pode gerenciar configurações de aplicativos e desktops, como políticas e configurações de gerenciamento de energia.

  Pode ver os consoles **Gerenciar** e **Monitorar** no Studio. Você pode alterar o escopo.

> **Nota:**
>
> Para alterar o nome de exibição de um desktop como Administrador de Grupo de Entrega, você precisa da permissão **Executar Atualização de Máquina**. Essa permissão é necessária porque a alteração do nome de exibição envolve a atualização da propriedade da máquina.

- **Administrador de Host:** Pode gerenciar conexões de host e suas configurações de recursos associadas. Não pode entregar máquinas, aplicativos ou desktops a usuários.

  Pode ver o console **Gerenciar** no Studio. Não pode ver o console **Monitorar**. Você pode alterar o escopo.
- **Administrador de Sessão:** Pode visualizar grupos de entrega sendo monitorados e gerenciar suas sessões e máquinas associadas.

  Pode ver o console **Monitorar** no Studio. Não pode ver o console **Gerenciar**. Você não pode alterar o escopo.
- **Administrador de Monitoramento Completo:** Pode executar todas as tarefas e operações para monitorar o DaaS.

  Pode ver o console **Monitorar** no Studio. Não pode ver o console **Gerenciar**. Você não pode alterar o escopo.
- **Administrador de Agente de Sonda:** Tem acesso às APIs do Agente de Sonda.

  Pode ver os consoles **Gerenciar** e **Monitorar** no Studio. Tem acesso somente leitura à página **Aplicativos**, mas não pode acessar outras visualizações.

A tabela a seguir resume quais guias do console são visíveis para cada função de acesso personalizada no Citrix DaaS e se a função pode ser usada com escopos personalizados.

FUNÇÃO DE ADMINISTRADOR DE ACESSO PERSONALIZADO	PODE VER O CONSOLE GERENCIAR NO STUDIO?	PODE VER O CONSOLE MONITORAR NO STUDIO?	A FUNÇÃO PODE SER USADA COM ESCOPOS PERSONALIZADOS?
Administrador da Nuvem	Sim	Sim	Não

FUNÇÃO DE ADMINISTRADOR DE ACESSO PERSONALIZADO	PODE VER O CONSOLE GERENCIAR NO STUDIO?	PODE VER O CONSOLE MONITORAR NO STUDIO?	A FUNÇÃO PODE SER USADA COM ESCOPOS PERSONALIZADOS ?
Administrador Somente Leitura	Sim	Sim	Sim
Administrador de Suporte Técnico	Não	Sim	Não
Administrador de Catálogo de Máquinas	Sim	Sim	Sim
Administrador de Grupo de Entrega	Sim	Sim	Sim
Administrador de Host	Sim	Não	Sim
Administrador de Sessão	Não	Sim	Não
Administrador de Monitoramento Completo	Não	Sim	Não
Administrador de Agente de Sonda	Sim	Sim	Não

Nota:

- Funções de administrador de acesso personalizado (exceto Administrador de Nuvem e Administrador de Help Desk) não estão disponíveis para Virtual Apps Essentials e Virtual Desktops Essentials.
- Funções de administrador de acesso personalizado (exceto Administrador de Nuvem e Administrador de Monitoramento Completo) não estão disponíveis para Citrix DaaS Standard for Azure.

> Para visualizar as permissões associadas a uma função:

1. Faça login em Citrix Cloud.
2. No bloco **DaaS**, clique em **Gerenciar** para abrir o Studio.
3. No painel esquerdo, selecione **Gerenciar > Administradores**.
4. Selecione a guia **Funções**.
5. Selecione uma função no painel superior central. A guia **Definição de função** no painel inferior lista as categorias e permissões. Selecione uma categoria para ver as permissões específicas. A guia **Administradores** lista os administradores que receberam a função selecionada.

Quantos administradores você precisa

O número de administradores e a granularidade de suas permissões geralmente dependem do tamanho e da complexidade da implantação.

- Em implantações pequenas ou de prova de conceito, um ou poucos administradores fazem tudo. Não há delegação de acesso personalizada. Nesse caso, cada administrador tem acesso total, que sempre tem o escopo Todos.
- Em implantações maiores com mais máquinas, aplicativos e desktops, é necessária mais delegação. Vários administradores podem ter responsabilidades funcionais mais específicas (funções). Por exemplo, dois têm acesso total e outros são administradores de suporte técnico. Além disso, um administrador pode gerenciar apenas certos grupos de objetos (escopos), como catálogos de máquinas em um departamento específico. Nesse caso, crie novos escopos, além de administradores com a função de acesso personalizado e escopos apropriados.

Resumo do gerenciamento de administradores

A configuração de administradores para o Citrix DaaS segue esta sequência:

1. Se você quiser que o administrador tenha uma função diferente de uma função interna, crie uma função personalizada.
2. Se você quiser que o administrador tenha um escopo diferente de Todos (e um escopo diferente for permitido para a função pretendida e ainda não tiver sido criado), crie escopos.
3. No Citrix Cloud, convide um administrador. Se você quiser que o novo administrador tenha algo diferente do acesso total padrão, especifique um par de função de acesso personalizado e escopo.

Mais tarde, se você quiser alterar o acesso de um administrador (funções e escopo), consulte Configurar acesso personalizado.

Adicionar um administrador

Para adicionar (convidar) administradores, siga as orientações em Adicionar administradores a uma conta Citrix Cloud. Um subconjunto dessas informações é repetido aqui.

> **Importante:**

> Não confunda como "personalizado" e "acesso personalizado" são usados.

> - Ao criar administradores e atribuir funções para o Citrix DaaS no console do Citrix Cloud, o termo "acesso personalizado" inclui tanto as funções integradas quanto quaisquer funções personalizadas adicionais que foram criadas na interface do Studio do serviço.
> - Na interface do Studio do serviço, "personalizado" simplesmente diferencia essa função de uma função integrada.

> O fluxo de trabalho geral para adicionar administradores é o seguinte:

1. Faça login no Citrix Cloud e selecione **Gerenciamento de Identidade e Acesso** no menu superior esquerdo.
2. Na página **Gerenciamento de Identidade e Acesso**, selecione **Administradores**. A guia **Administradores** lista todos os administradores atuais da conta.
3. Na guia **Administradores**, selecione seu tipo de identidade, insira o endereço de e-mail do administrador e clique em **Convidar**.

- Selecione **Acesso total** se desejar que o administrador tenha acesso total. Dessa forma, o administrador pode acessar todas as funções de administrador do cliente no Citrix Cloud e em todos os serviços assinados.
- Selecione **Acesso personalizado** se desejar que o administrador tenha acesso limitado. Você pode então selecionar um par de função e escopo de acesso personalizado. Dessa forma, o administrador terá as permissões pretendidas ao fazer login no Citrix Cloud.

1. Clique em **Enviar Convite**. O Citrix Cloud envia um convite para o endereço de e-mail e adiciona o administrador à lista depois que o administrador conclui o processo de integração.

Ao receber o e-mail, o administrador clica no link **Entrar** para aceitar o convite.

Para obter mais informações sobre como adicionar administradores, consulte Gerenciar administradores do Citrix Cloud.

Alternativamente, vá para **Administradores > Administradores** no Studio e clique em **Adicionar Administrador**. Você será levado diretamente para **Gerenciamento de Identidade e Acesso > Administradores**, que se abre em uma nova guia do navegador. Depois de terminar de adicionar administradores lá, feche a guia e retorne ao console para continuar com suas outras tarefas de configuração.

Criar e gerenciar funções

Quando os administradores criam ou editam uma função, eles podem habilitar apenas as permissões que eles próprios possuem. Esse controle impede que os administradores criem uma função com mais permissões do que eles têm atualmente e a atribuam a si mesmos (ou editem uma função à qual já estão atribuídos).

Os nomes de funções personalizadas podem conter até 64 caracteres Unicode. Os nomes não podem conter: barra invertida, barra, ponto e vírgula, dois pontos, cerquilha, vírgula, asterisco, ponto de interrogação, sinal de igual, seta para a esquerda, seta para a direita, pipe, colchete esquerdo ou direito, parêntese esquerdo ou direito, aspas e apóstrofo.

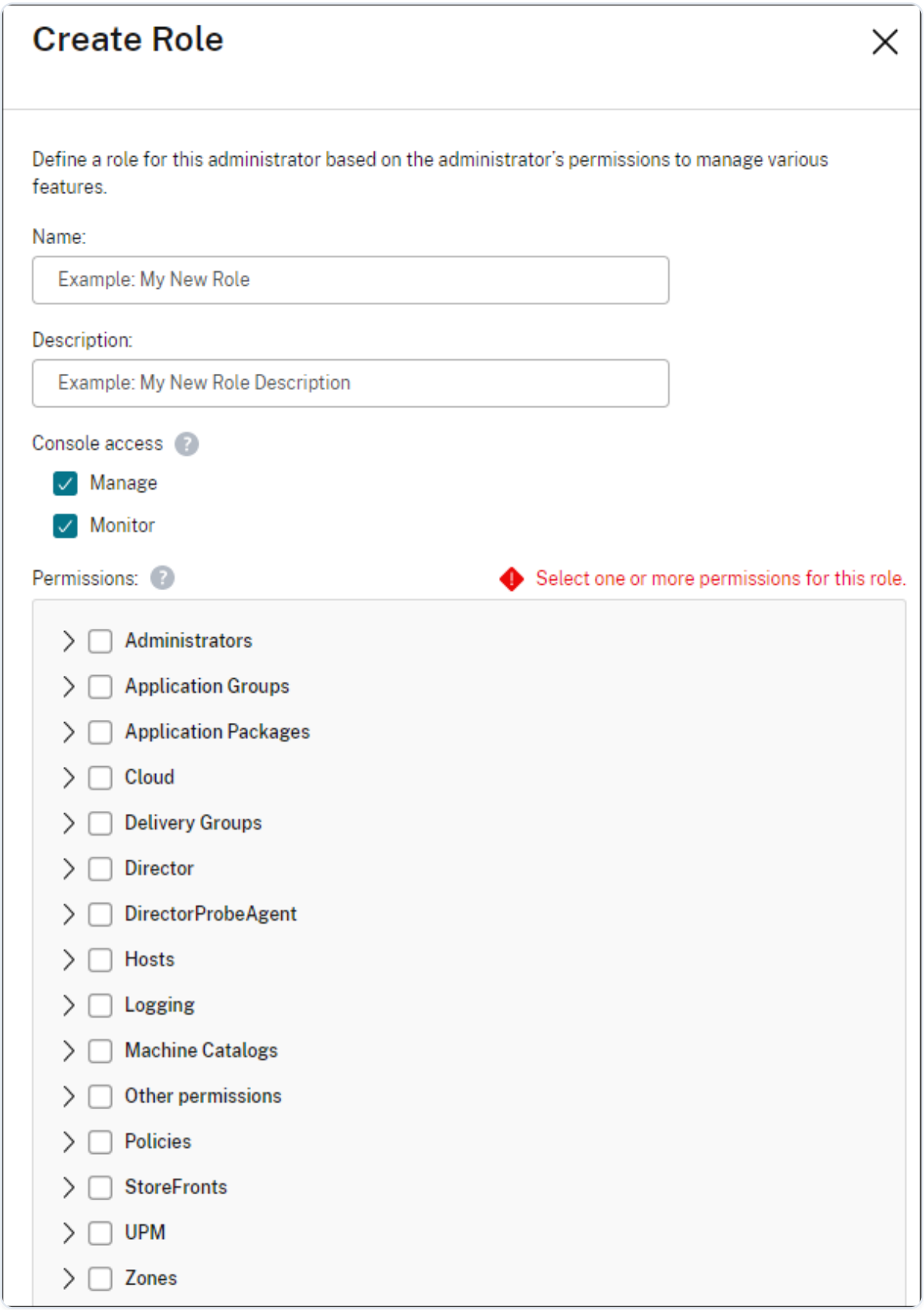
As descrições de funções podem conter até 256 caracteres Unicode.

1. Faça login no Citrix Cloud se ainda não o fez.
2. No bloco **DaaS**, clique em **Gerenciar** para abrir o Studio.
3. No painel esquerdo, selecione **Gerenciar > Administradores**.
4. Selecione a guia **Funções**.
5. Siga as instruções para a tarefa que deseja concluir:

    - **Exibir detalhes da função:** Selecione a função no painel central. A parte inferior do painel central lista os tipos de objeto e as permissões associadas à função. Selecione a guia **Administradores** no painel inferior para exibir uma lista de administradores que atualmente possuem esta função.
    - **Criar uma função personalizada:** Selecione **Criar Função** na barra de ações. Configure as definições da seguinte forma:

        - Insira um nome e uma descrição.

- Configure o acesso ao console. Determine quais consoles são visíveis para os administradores. Você pode prosseguir sem selecionar nenhum console. Nesse caso, os administradores com a função não podem acessar **Gerenciar** e **Monitorar**, mas podem acessar, visualizar ou gerenciar objetos por meio de SDKs e APIs.
- Selecione os tipos de objeto e as permissões. Para conceder permissão de acesso total a um tipo de objeto, selecione sua caixa de seleção. Para conceder permissão em um nível granular, expanda o tipo de objeto e, em seguida, selecione **Somente Leitura** ou objetos individuais em **Gerenciar** dentro do tipo.



- **Copiar uma função:** Selecione a função no painel central e, em seguida, selecione **Copiar Função** na barra de ações. Altere o nome, a descrição, os tipos de objeto e as permissões, conforme necessário. Quando terminar, selecione **Salvar**.

- **Editar uma função personalizada:** Selecione a função no painel central e, em seguida, selecione **Editar Função** na barra de ações. Altere o nome, a descrição, os tipos de objeto e as permissões, conforme necessário. Você não pode editar uma função integrada. Quando terminar, selecione **Salvar**.
- **Excluir uma função personalizada:** Selecione a função no painel central e, em seguida, selecione **Excluir Função** na barra de ações. Quando solicitado, confirme a exclusão. Você não pode excluir uma função integrada. Você não pode excluir uma função personalizada se ela estiver atribuída a um administrador.

Criar e gerenciar escopos

Por padrão, todas as funções têm o escopo Todos para seus objetos relevantes. Por exemplo, um Administrador de Grupo de Entrega pode gerenciar todos os Grupos de Entrega. Para algumas funções de administrador, você pode criar um escopo que permite que essa função de administrador acesse um subconjunto dos objetos relevantes. Por exemplo, você pode querer dar a um Administrador de Catálogo de Máquinas acesso apenas a catálogos que contêm um certo tipo de máquinas, em vez de todos os catálogos.

- Administradores de acesso total ou Administradores de Nuvem de acesso personalizado podem criar escopos para as funções de Administrador Somente Leitura, Administrador de Catálogo de Máquinas, Administrador de Grupo de Entrega e Administrador de Host.
- Escopos não podem ser criados para administradores de acesso total, nem podem ser criados para Administradores de Nuvem ou Administradores de Help Desk. Esses administradores sempre têm o escopo Todos.

Criar escopos

1. No Studio, selecione **Gerenciar > Administradores** no painel esquerdo.
2. Selecione a guia **Escopos**.
3. Na barra de ações, selecione **Criar Escopo**.
4. Insira um nome e uma descrição:
    - Os nomes de escopo podem conter até 64 caracteres Unicode. Os nomes não podem incluir: barra invertida, barra, ponto e vírgula, dois pontos, cerquilha, vírgula, asterisco, ponto de interrogação, sinal de igual, seta para a esquerda ou para a direita, pipe, colchete esquerdo ou direito, parêntese esquerdo ou direito, aspas e apóstrofo.
    - As descrições de escopo podem conter até 256 caracteres Unicode.

5. Selecione os objetos que você deseja incluir neste escopo. Os objetos são listados por tipo, como grupos de entrega e catálogos de máquinas.

   - Para incluir todos os objetos de um tipo específico (por exemplo, todos os grupos de entrega), selecione a caixa de seleção para o tipo de objeto.
   - Para incluir objetos individuais dentro de um tipo, expanda o tipo e, em seguida, selecione as caixas de seleção para os objetos (por exemplo, grupos de entrega específicos).

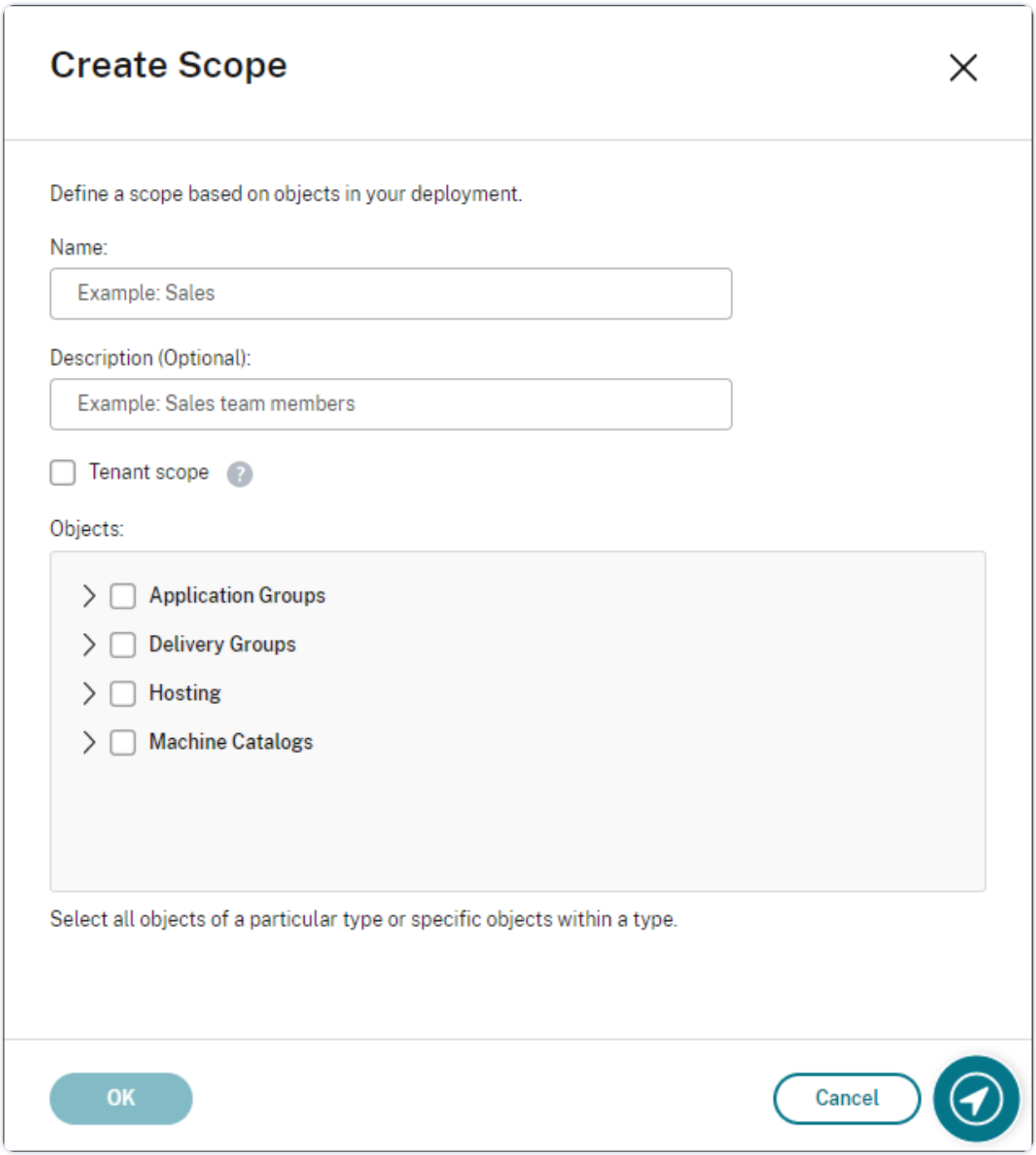
     > **Nota:**
     >
     > Grupos de aplicativos, grupos de entrega ou catálogos de máquinas são exibidos em estruturas de pastas que se alinham com seu gerenciamento no DaaS. Você pode selecionar uma pasta para selecionar todos os seus objetos ou expandir uma pasta para selecionar objetos específicos.

   - Para incluir um objeto que anteriormente não suportava o controle de escopo (um objeto *não escopado*) e agora o suporta (um objeto *escopado*), desabilite **Ignorar controle de escopo** ao lado do objeto e, em seguida, selecione-o.

     > **Nota:**
     >
     > Objetos *não escopados* são visíveis para todos os administradores com as permissões necessárias. Quando tal objeto se torna *escopado*, **Ignorar controle de escopo** aparece e é habilitado por padrão para preservar a visibilidade para todos os administradores.

   - Para criar um cliente locatário, selecione a caixa de seleção **Escopo do locatário**. Se selecionado, o nome que você inseriu para o escopo é o nome do locatário. Para obter mais informações sobre o escopo do locatário, consulte Gerenciar locatários.

6. Quando terminar, selecione **OK**.



Depois de criar um escopo, ele aparece na lista **Acesso personalizado** no console do Citrix Cloud. Você pode então selecioná-lo ao atribuir uma função a um administrador.

Por exemplo, se você criar um escopo chamado **CAD** e incluir catálogos com máquinas adequadas para aplicativos CAD, o escopo **CAD** aparecerá na lista **Editar escopos** ao atribuir funções no console do Citrix Cloud.

> **Nota:**

> As funções de **Administrador da Nuvem** e **Administrador de Suporte Técnico** sempre têm o escopo **Todos**. O escopo CAD não se aplica a elas.

Gerenciar escopos

Você pode realizar as seguintes tarefas para gerenciar escopos:

- **Exibir detalhes do escopo:** Selecione o escopo. A parte inferior do painel lista os objetos e administradores que possuem esse escopo.
- **Copiar um escopo:** Selecione o escopo no painel central e, em seguida, selecione **Copiar Escopo** na barra de ações. Altere o nome e a descrição. Altere os tipos de objeto e os objetos, conforme necessário. Quando terminar, selecione **Salvar**.
- **Editar um escopo:** Selecione o escopo no painel central e, em seguida, selecione **Editar Escopo** na barra de ações. Altere o nome, a descrição, os tipos de objeto e os objetos, conforme necessário. Quando terminar, selecione **Salvar**.

  > **Nota:**
  >
  > Ao copiar ou editar um escopo, lembre-se de que a remoção de objetos do escopo pode torná-los inacessíveis a um administrador. Se o escopo editado estiver emparelhado com uma ou mais funções, certifique-se de que suas atualizações de escopo não tornem nenhum par função/escopo inutilizável.

- **Excluir um escopo:** Selecione o escopo no painel central e, em seguida, selecione **Excluir Escopo** na barra de ações. Quando solicitado, confirme a exclusão.

  Você não pode excluir um escopo se ele estiver atribuído a uma função. Se você tentar fazer isso, uma mensagem de erro indicará que você não tem permissão. Na verdade, o erro ocorre porque o par função/escopo que usa este escopo está atribuído a um administrador. Primeiro, remova a atribuição do par função/escopo para todos os administradores que o utilizam. Em seguida, exclua o escopo no Studio.

Gerenciar locatários

Usando o Studio, você pode criar locatários mutuamente exclusivos em um único Citrix DaaS. Você consegue isso criando escopos de locatário em **Administradores > Escopos** e associando objetos de configuração relacionados, como catálogos de máquinas e grupos de entrega, a esses

locatários. Como resultado, os administradores com acesso a um locatário podem gerenciar apenas os objetos associados a esse locatário.

Esse recurso é útil, por exemplo, se sua organização:

- Possui diferentes silos de negócios (divisões independentes ou equipes de gerenciamento de TI separadas) ou
- Possui vários sites locais e deseja manter a mesma configuração em uma única instância do Citrix DaaS.

A interface permite filtrar clientes locatários por nome. Por padrão, a interface exibe informações sobre todos os clientes locatários. Para exibir informações sobre um locatário específico, selecione esse locatário na lista no canto superior direito.

Criar um cliente locatário

Para criar um cliente de locatário, selecione **Escopo de locatário** ao criar um escopo. Ao selecionar a opção, você cria um tipo de escopo exclusivo que se aplica a objetos em cenários onde você compartilha uma instância do Citrix DaaS entre diferentes unidades de negócios — cada uma dessas unidades de negócios é independente das outras. Depois de criar um escopo de locatário, você não pode alterar o tipo de escopo.

Criar um cliente de locatário(/en-us/citrix-daas/media/create-a-tenant-customer.png)

A guia **Escopos** exibe todos os itens de escopo. A única diferença entre escopos regulares e escopos de locatário está na coluna **Tipo**. Um campo de coluna em branco indica um escopo regular. Você pode clicar na coluna **Tipo** para classificar os itens de escopo, se necessário.

Para ver os recursos (objetos) anexados a um escopo, selecione **Administradores** no painel esquerdo. Na guia **Escopos**, selecione o escopo e, em seguida, selecione **Editar Escopo** na barra de ações.

> **Dica:**

> A propriedade de locatário é atribuída no nível do escopo. Catálogos de máquinas, grupos de entrega, aplicativos e conexões herdam a propriedade de locatário do escopo aplicável.

> Ao usar um escopo de locatário, esteja ciente das seguintes considerações:

- A propriedade de locatário é atribuída na seguinte ordem: **Hospedagem > Catálogos de Máquinas > Grupos de Entrega > Aplicativos**. Objetos de nível inferior dependem de objetos de nível superior para herdar a propriedade de locatário. Por exemplo, ao selecionar um grupo de entrega, você deve selecionar a hospedagem e o catálogo de máquinas associados. Caso contrário, o grupo de entrega não poderá herdar a propriedade de locatário.
- Após criar um escopo de locatário, você pode editar as atribuições de locatário modificando objetos. Quando uma atribuição de locatário é alterada, ela ainda está sujeita à restrição de que deve ser atribuída aos mesmos locatários ou a um subconjunto desses locatários. No entanto, objetos de nível inferior não são reavaliados quando as atribuições de locatário mudam. Certifique-se de que os objetos estejam devidamente restritos ao alterar as atribuições de locatário. Por exemplo, se um catálogo de máquinas estiver disponível para `TenantA` e `TenantB`, você pode criar um grupo de entrega para `TenantA` e outro para `TenantB`. (`TenantA` e `TenantB` estão ambos associados a esse catálogo de máquinas.) Você pode então alterar o catálogo de máquinas para ser associado apenas a `TenantA`. Como resultado, o grupo de entrega associado a `TenantB` se torna inválido.

Configurar acesso personalizado para administradores

Após criar escopos de locatário, configure o acesso personalizado para os respectivos administradores. Para obter mais informações, consulte Configurar acesso personalizado para um administrador. O Citrix Cloud envia um convite para os administradores de cliente que você especificou e os adiciona à lista. Ao receberem o e-mail, eles clicam em **Entrar** para aceitar o convite. Ao fazerem login no Studio, eles veem os recursos que os pares de função e escopo atribuídos contêm.

Configurar acesso personalizado para clientes de locatário(/en-us/citrix-daas/media/configure-custom-access-for-tenants.png)

Administradores com acesso a um locatário podem gerenciar apenas objetos (por exemplo, catálogo de máquinas, grupo de entrega) que estão associados ao locatário.

Configurar acesso personalizado para um administrador

Este recurso permite definir permissões de acesso de administradores existentes ou administradores que você convida de uma forma que se alinha com sua função em sua organização.

As alterações feitas nas permissões de acesso levam 5 minutos para entrar em vigor. Sair do Studio e fazer login novamente faz com que as alterações entrem em vigor imediatamente. Em cenários em que os administradores ainda usam a interface de gerenciamento depois que as

alterações entram em vigor sem se reconectar a ela, um aviso aparece quando eles tentam acessar itens para os quais não têm mais permissões.

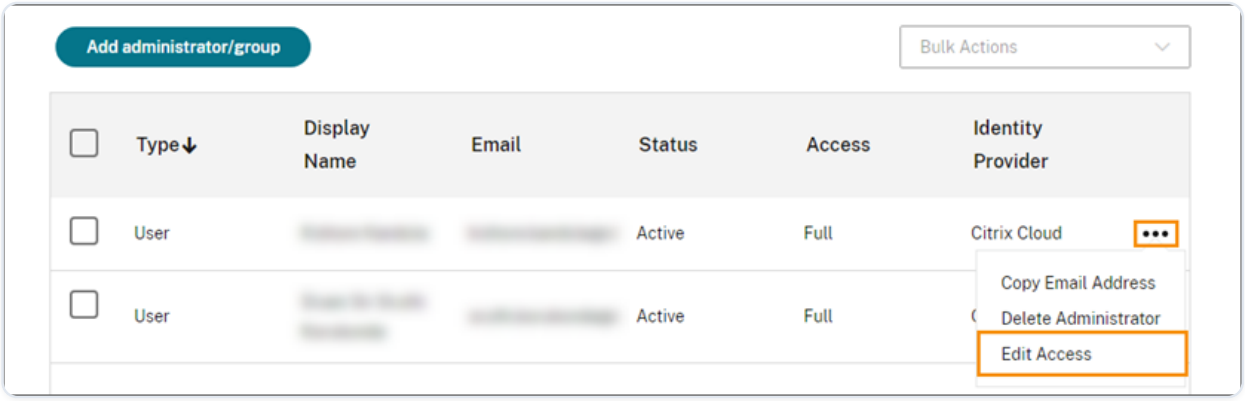
Por padrão, ao convidar administradores, eles têm acesso total. O acesso total permite que o administrador gerencie todos os serviços assinados e todas as operações do Citrix Cloud (como convidar mais administradores). Uma implantação do Citrix Cloud precisa de pelo menos um administrador com acesso total.

Você também pode conceder acesso personalizado ao convidar um administrador. O acesso personalizado permite que o administrador gerencie apenas os serviços e operações que você especificar.

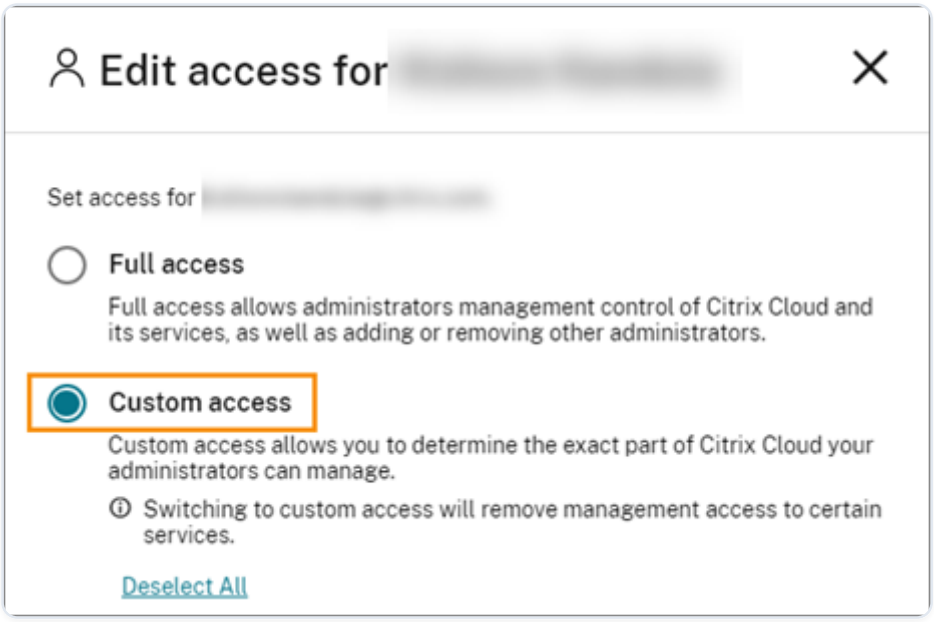
Ao criar uma função ou escopo no Citrix DaaS, ele aparece na lista de acesso personalizado e pode ser selecionado. Ao selecionar uma função para um administrador, você pode modificar os escopos conforme necessário para refletir a função do administrador em sua organização.

Para configurar o acesso personalizado para um administrador:

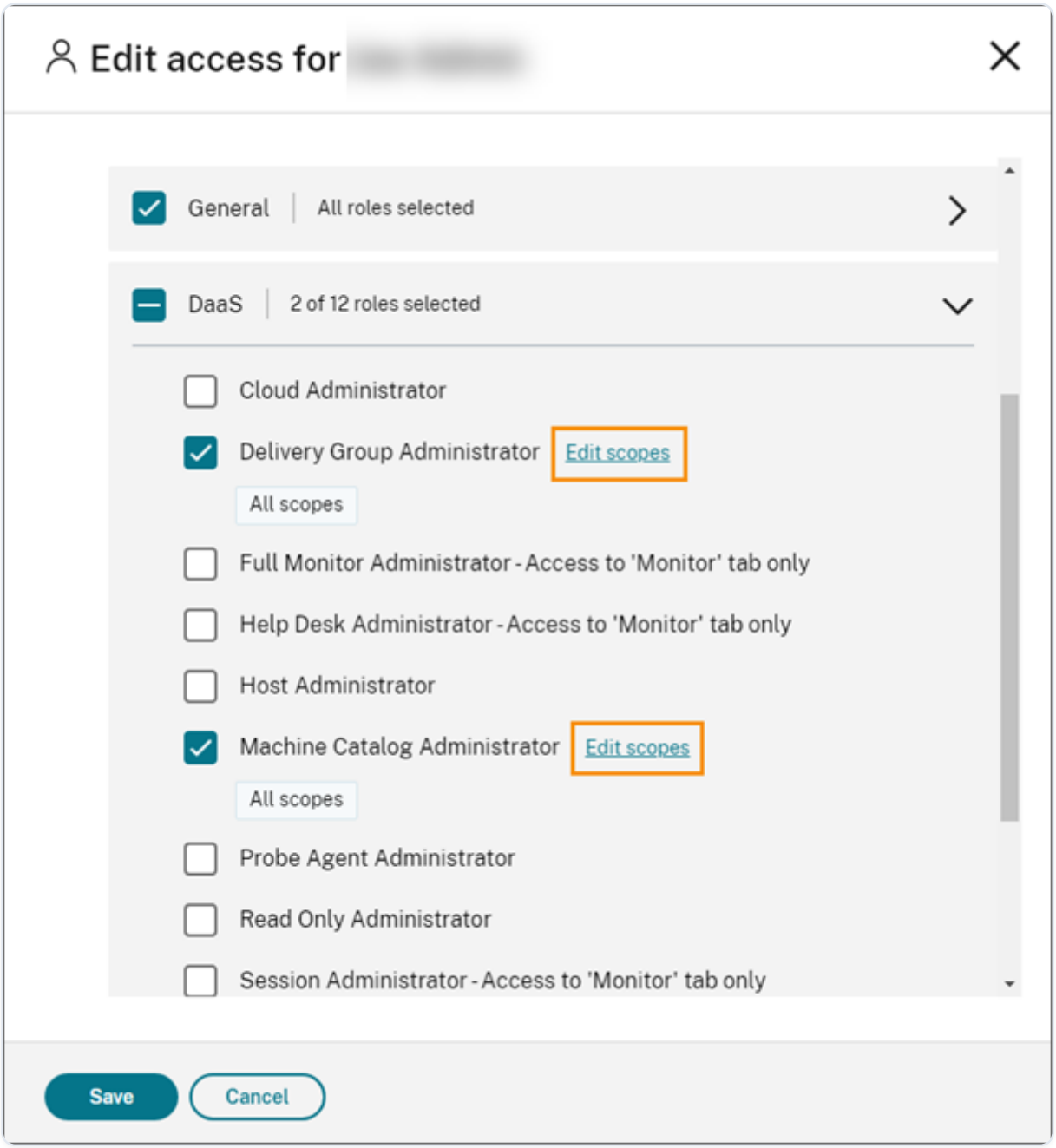
1. Faça login no Citrix Cloud. Selecione **Gerenciamento de Identidade e Acesso** > **Administradores** no menu superior esquerdo.
2. Localize o administrador que você deseja gerenciar, selecione o menu de reticências e selecione **Editar acesso**.



3. Selecione **Acesso personalizado**.

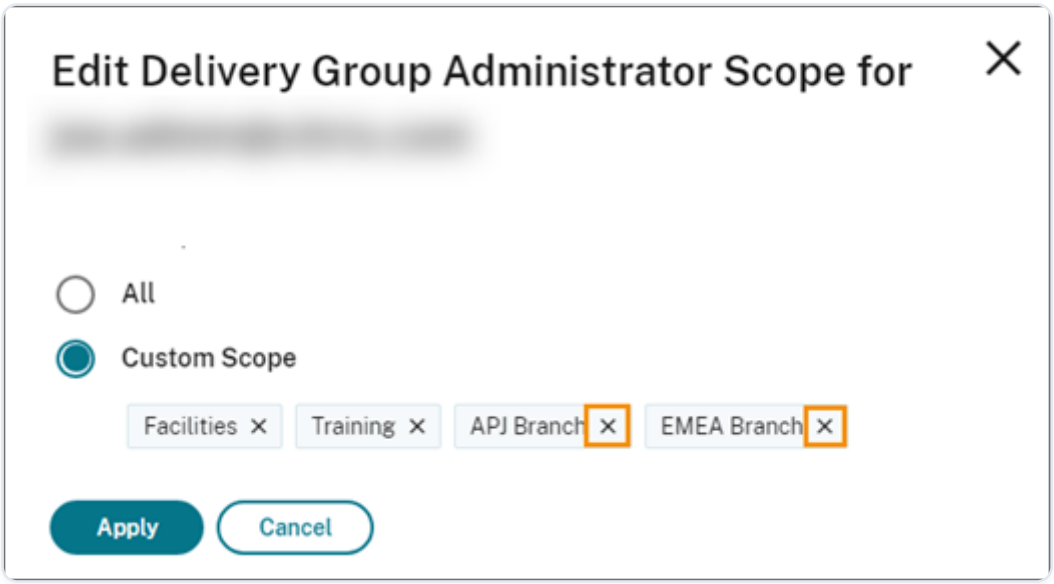


4. Em **DaaS**, selecione ou desmarque as caixas de seleção ao lado de uma ou mais funções. Para modificar os escopos associados a uma função atribuída, selecione **Editar escopos**.

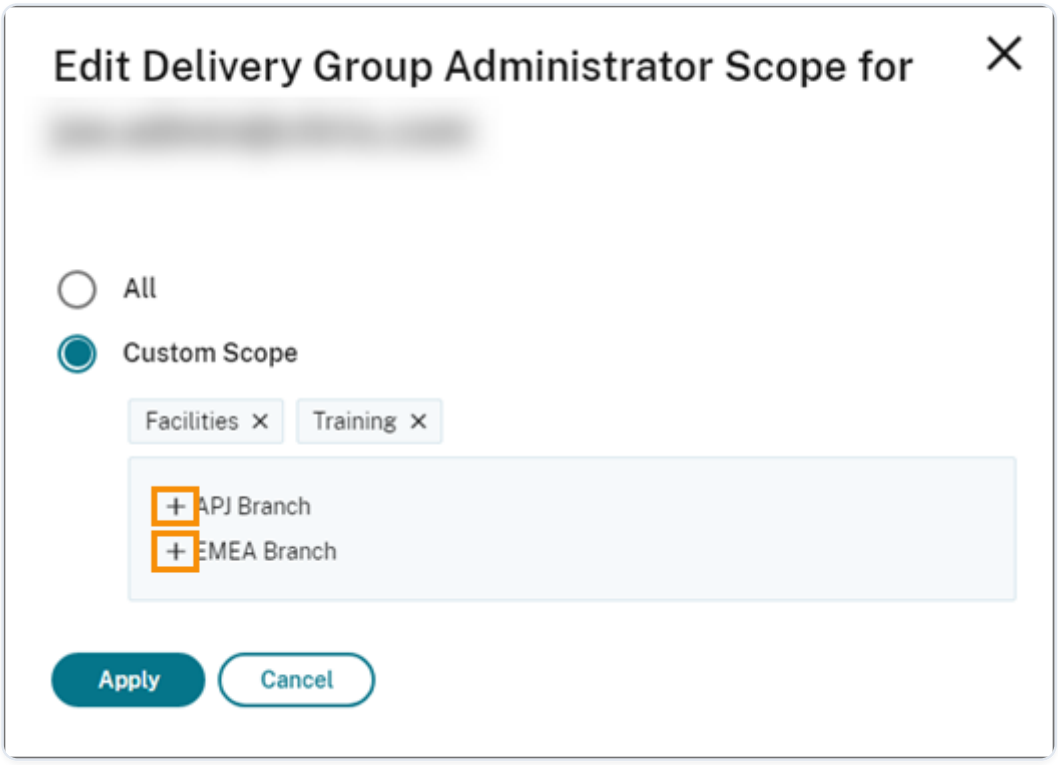


Por padrão, cada função selecionada tem todos os escopos selecionados, conforme indicado pelo rótulo **Todos os escopos**.

5. Para especificar os escopos para uma função selecionada, selecione **Escopo Personalizado** e, em seguida, adicione ou remova os escopos apropriados. Por padrão, todos os escopos personalizados são adicionados a uma função. Para remover um escopo, clique no ícone X no escopo.



Escopos que foram removidos e estão disponíveis para adicionar à função aparecem em uma lista abaixo dos escopos que já foram adicionados. Para adicionar um escopo à função, selecione o ícone de adição para o escopo.



6. Quando terminar de selecionar os escopos, selecione **Aplicar**.
7. Selecione **Salvar** para salvar as funções selecionadas para o administrador.

Diferenças em relação ao Citrix Virtual Apps and Desktops local

Se você está familiarizado com a administração delegada no produto Citrix Virtual Apps and Desktops local, a versão do Citrix DaaS apresenta várias diferenças.

No Citrix Cloud:

- Os administradores são identificados pelo seu login no Citrix Cloud, em vez de sua conta do Active Directory. Você pode criar pares de função/escopo para indivíduos do Active Directory, mas não para grupos.
- Os administradores são criados, configurados e excluídos no console do Citrix Cloud, em vez de no Citrix DaaS.
- Os pares de função/escopo são atribuídos aos administradores no console do Citrix Cloud, em vez de no Citrix DaaS.
- Os relatórios não estão disponíveis. Você pode visualizar informações de administrador, função e escopo na interface do Studio do serviço.
- O Administrador de Nuvem de acesso personalizado é semelhante a um Administrador Completo na versão local. Ambos possuem permissões completas de gerenciamento e monitoramento para a versão do Citrix Virtual Apps and Desktops em uso.

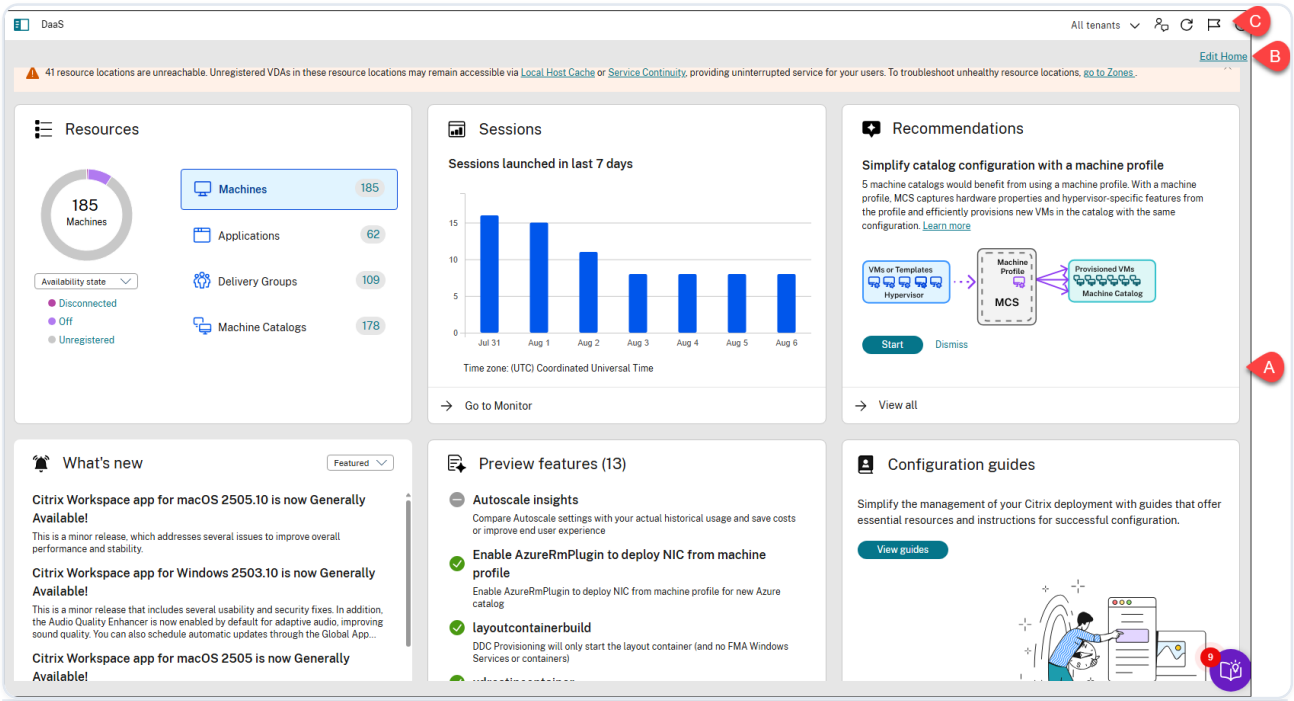
  No entanto, no Citrix DaaS, não há uma função de Administrador Completo nomeada. Não equipare "Acesso total" no Citrix Cloud com o "Administrador completo" no Citrix Virtual Apps and Desktops local. O acesso total no Citrix Cloud abrange os domínios de nível de plataforma, biblioteca, notificações e locais de recursos, além de todos os serviços assinados.

Mais informações

Consulte Administração e monitoramento delegados para obter informações sobre administradores, funções e escopos usados no nó **Monitor** do serviço.

Página inicial

A página inicial do Studio fornece uma visão geral da sua implantação e cargas de trabalho do Citrix DaaS™ juntamente com informações que o ajudam a aproveitar ao máximo sua assinatura. Este artigo apresenta os widgets disponíveis nesta página.



CHAMADA	ÁREA	DESCRIÇÃO
A	Widgets	Fornece uma visão geral da sua implantação e cargas de trabalho do Citrix DaaS, juntamente com informações que o ajudam a aproveitar ao máximo sua assinatura. Os widgets incluem Recursos, Sessões, Recomendações, Novidades, Recursos de visualização, Guias de configuração, Erros e avisos e Consultor.
B	Ação Editar Página Inicial	Permite que você personalize a página inicial adicionando, removendo ou reposicionando widgets.
C	Alertas de integridade do serviço (ícone de bandeira)	Exibe alertas relacionados à integridade do seu site.

Recursos

Este widget fornece uma visão geral da sua implantação do Citrix DaaS:

- **Recursos**. Mostra o número de recursos implantados e suas contagens por categoria.

RECURSO	PARA VISUALIZAR CONTAGENS POR CATEGORIA
Máquinas	Clique em **Máquinas**, selecione um estado e, em seguida, passe o mouse sobre o gráfico de rosca para obter detalhes. Opções disponíveis: **Estado de disponibilidade** (Disponível, Em uso, Desligado e Indisponível), **Estado de registro** (Registrado e Não registrado) e **Estado de manutenção** (Em manutenção e Não em manutenção). Ao visualizar as contagens de máquinas por estado de disponibilidade, você pode clicar em um estado para visualizar os detalhes correspondentes da máquina.
Aplicativos	Clique em **Aplicativos** e passe o mouse sobre o gráfico de rosca para obter detalhes.
Grupos de Entrega	Clique em **Grupos de Entrega** e passe o mouse sobre o gráfico de rosca para obter detalhes.
Catálogos de Máquinas	Clique em **Catálogos de Máquinas** e passe o mouse sobre o gráfico de rosca para obter detalhes.

- **Sessões iniciadas nos últimos 7 dias**. Mostra o número de sessões de desktop e aplicativos iniciadas a cada dia nos últimos sete dias. Para detalhar e obter mais informações, clique em Ir para Monitor.

Sessões

Este widget fornece uma visão geral das suas cargas de trabalho do Citrix DaaS nos últimos 7 dias. Mostra o número de sessões de desktop e aplicativos iniciadas diariamente nos sete dias anteriores. Para detalhar e obter mais informações, clique em Ir para Monitor.

Recomendações

Este widget recomenda recursos disponíveis com sua assinatura, como Workspace Environment Management e Autoscale. Para interagir conosco, curta ou não curta uma recomendação e deixe seu feedback.

> **Nota:**
>
> Se você não gostar de uma recomendação, ela desaparecerá. Se você não gostar de todas as recomendações ou do widget de recomendação, o widget de recomendação desaparecerá.

Novidades

Este widget mostra uma lista selecionada dos recursos mais recentes do Citrix DaaS que são mais valiosos para o seu negócio. Usar esses recursos ajuda você a aproveitar ao máximo sua assinatura. Para uma lista completa de novos recursos, consulte Novidades.

Recursos de visualização

Este widget mostra recursos que estão atualmente em visualização. Como administrador do Citrix Cloud™ com acesso total, você pode ativar ou desativar os recursos de visualização sem entrar em contato com a Citrix. Leva até 15 minutos para que as alterações entrem em vigor.

Os recursos de visualização são recomendados para uso em ambientes que não sejam de produção. Problemas encontrados com recursos de visualização não são suportados pelo Suporte Técnico da Citrix.

Guias de configuração

Este widget fornece orientação passo a passo para configurar e gerenciar vários aspectos da sua implantação Citrix:

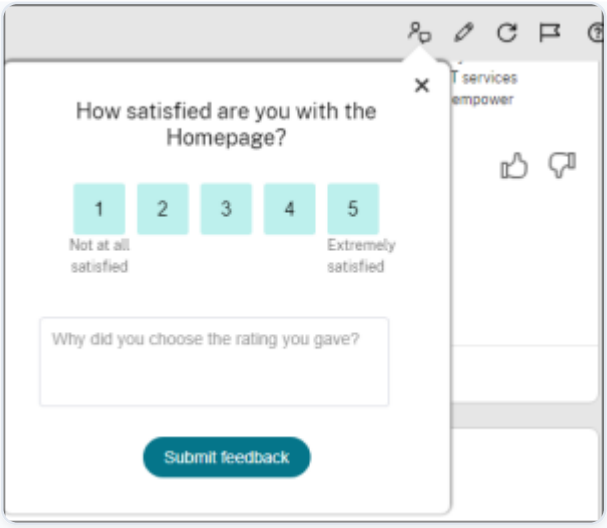
- **Comece a usar o DaaS**. Orienta você por uma série de perguntas para ajudar a configurar suas implantações DaaS. Ao responder a essas perguntas, você pode configurar rapidamente suas implantações. Para obter mais informações, consulte Usar o guia de introdução do DaaS.
- **Verificar configurações de resiliência**. Orienta você na verificação de que sua implantação do Citrix DaaS está configurada corretamente para manipular interrupções potenciais. Este guia fornece listas de verificação para verificar se os componentes chave, como Local Host Cache e Service Continuity, estão configurados corretamente. Essa verificação ajuda a

garantir acesso ininterrupto a aplicativos e desktops durante interrupções de serviço. Inclui listas de verificação para verificar as configurações de resiliência em vários tipos de implantação do StoreFront™:

- Lista de verificação para implantações locais do Citrix® StoreFront
- Lista de verificação para implantações do Citrix® StoreFront Cloud
- Lista de verificação para implantações mistas do StoreFront

Nota:

A lista de verificação de resiliência não é uma tarefa única. Nós o encorajamos a revisar regularmente sua prontidão de resiliência testando a Continuidade do Serviço e o Cache do Host Local. Se você tiver feedback sobre a lista de verificação, use o ícone de feedback no canto superior direito da página inicial para compartilhá-lo conosco.



Erros e avisos

Exibe centralizadamente erros e avisos de suas implantações DaaS:

- Lista o número de erros e o número de avisos presentes nos seguintes nós de configuração: Zonas, Máquinas, Catálogos de Máquinas, Grupos de Entrega, Hospedagem e Imagens. Clicar em um número o vincula à interface do usuário do nó correspondente.
- Lista os erros de alta prioridade em seu site, juntamente com as ações recomendadas.

Advisor

O widget **Advisor** exibe um resumo das recomendações da sua verificação de site mais recente do Advisor, dando a você visibilidade rápida da saúde do ambiente sem sair da página inicial.

O widget mostra:

- Uma contagem do total de recomendações agrupadas por nível de impacto: **Alto**, **Médio** e **Baixo**
- Um gráfico de barras visual mostrando a distribuição entre os níveis de impacto
- Uma lista filtrável de recomendações por categoria: **Segurança**, **Confiabilidade**, **Desempenho**, **Excelência Operacional** e **Otimização de Custos**
- Um carimbo de data/hora indicando quando o Advisor foi executado pela última vez

Você pode filtrar as recomendações selecionando uma categoria no menu suspenso. Selecione qualquer recomendação na lista para navegar diretamente para seus detalhes na página completa do **Advisor**. Selecione **Ir para o Advisor** para visualizar a interface completa do Advisor.

Se não houver resultados de verificação recentes disponíveis, o widget exibirá uma mensagem solicitando que você execute uma nova verificação do site.

Personalizar a página inicial

Para personalizar a página inicial, siga estas etapas:

1. Faça login no Citrix Cloud.
2. No bloco **DaaS**, clique em **Gerenciar**. A página inicial é exibida.
3. Clique no ícone **Editar** no canto superior direito da página inicial.
4. Para reposicionar um widget, arraste-o para a posição desejada.
5. Para remover um widget da página inicial, clique no ícone **Excluir** no canto superior direito do widget.
6. Para adicionar um widget de volta à página inicial, clique no ícone **Adicionar widget** no canto superior direito da página inicial.
7. Clique em **Concluído** para salvar as alterações.

Licenças

Este artigo aborda tarefas e recursos para licenças Microsoft e licenças Citrix®.

Configurar um Servidor de Licenças RDS da Microsoft para cargas de trabalho do Windows Server

Esta informação se aplica quando você está entregando cargas de trabalho do Windows Server.

Este serviço acessa os recursos de sessão remota do Windows Server ao entregar uma carga de trabalho do Windows Server, como o Windows 2019. Isso geralmente requer uma licença de acesso para cliente dos Serviços de Área de Trabalho Remota (RDS CAL). O VDA deve ser capaz de contatar um servidor de licenças RDS para solicitar RDS CALs.

Instale e ative o servidor de licenças. Para obter mais informações, consulte o documento da Microsoft Ativar o Servidor de Licenças dos Serviços de Área de Trabalho Remota. Para ambientes de prova de conceito, você pode usar o período de carência fornecido pela Microsoft.

Com este método, você pode fazer com que este serviço aplique as configurações do servidor de licenças. Você pode configurar o servidor de licenças e o modo por usuário no console RDS na imagem. Você também pode configurar o servidor de licenças usando as configurações de Política de Grupo da Microsoft. Para obter mais informações, consulte o documento da Microsoft Licenciar sua implantação RDS com licenças de acesso para cliente (CALs).

Para configurar o servidor de licenças RDS usando as configurações de Política de Grupo da Microsoft:

1. Instale um Servidor de Licenças dos Serviços de Área de Trabalho Remota em uma VM disponível. A VM deve estar sempre disponível. As cargas de trabalho do serviço Citrix devem ser capazes de alcançar este servidor de licenças.
2. Especifique o endereço do servidor de licenças e o modo de licença por usuário usando a Política de Grupo da Microsoft. Para obter detalhes, consulte o documento da Microsoft Especificar o Modelo de Licenciamento de Área de Trabalho Remota para um Servidor Host de Sessão RD.

As cargas de trabalho do Windows 10 exigem a ativação apropriada da licença do Windows 10. Recomendamos que você siga a documentação da Microsoft para ativar as cargas de trabalho do Windows 10.

Uso da licença Citrix

Para obter informações sobre o uso da licença Citrix, consulte:

- Monitorar licença e uso ativo para serviços em nuvem
- Monitorar licença e uso ativo para Citrix DaaS

Cache de Host Local

Este artigo fornece uma visão geral completa do recurso Cache de Host Local (LHC), com foco em sua capacidade de manter a continuidade dos negócios. Ele explica a funcionalidade do LHC tanto durante as operações normais de trabalho quanto quando o modo LHC é ativado. Além disso, o artigo oferece orientação sobre verificações de configuração, solução de problemas, comandos PowerShell para gerenciamento do LHC e monitoramento de log de eventos para a integridade do LHC.

Visão geral

O LHC mantém o acesso do usuário final a aplicativos e desktops quando os Cloud Connectors perdem a conectividade com o Citrix Cloud™ devido a uma interrupção de rede ou a um problema com o Citrix Cloud. As sessões ativas não são impactadas quando o modo LHC é ativado e novas sessões são intermediadas através do broker LHC em execução nos Cloud Connectors.

O LHC é habilitado por padrão, mas é importante garantir que seu ambiente esteja configurado corretamente para o LHC. Embora configurações incorretas possam não interromper a intermediação normal, elas podem prejudicar o desempenho do LHC, causando interrupção para os usuários finais quando o modo LHC está ativo. Para garantir a funcionalidade ideal do LHC, verifique seu nó Zonas no Studio para erros e avisos relacionados à zona que a Citrix detectou. Além disso, revise o guia Verificar configurações de resiliência e o artigo Evitar Configurações Incorretas Comuns que Podem Impactar Negativamente a Resiliência do DaaS para uma lista de verificação de configuração abrangente do LHC.

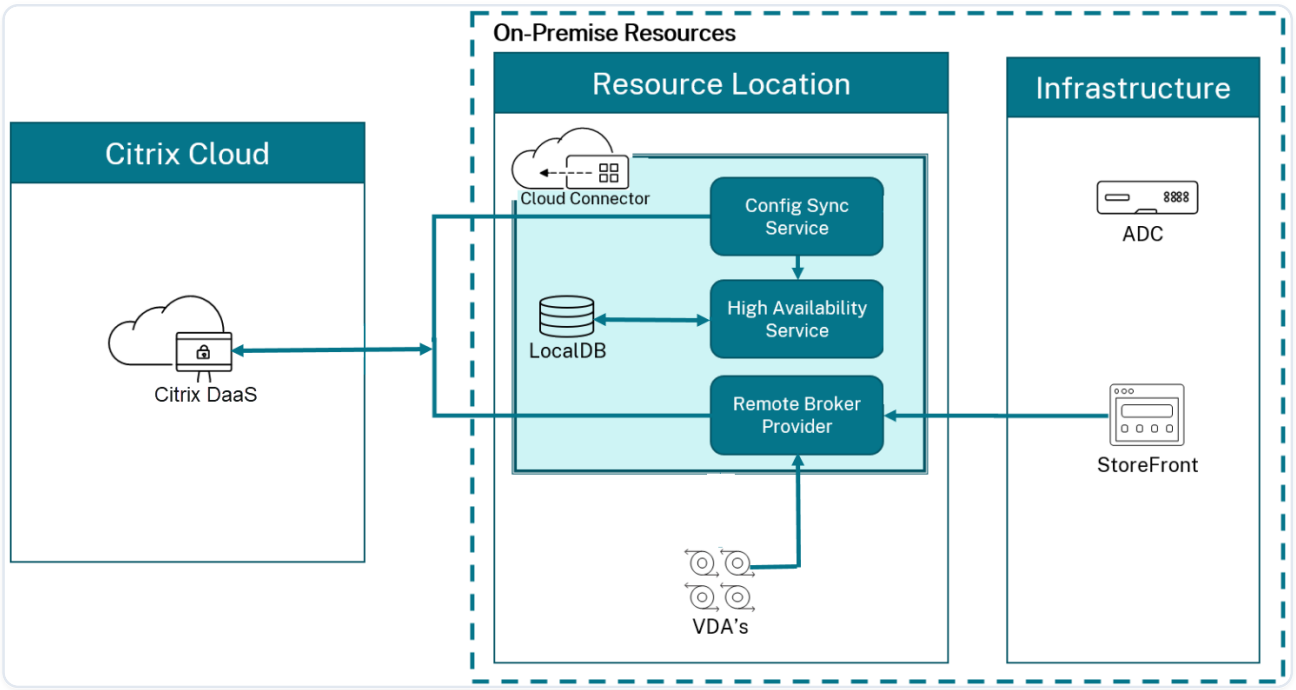
> **Importante:**
>
> O LHC só é ativado se os Cloud Connectors receberem tráfego do StoreFront ou se a Continuidade do Serviço estiver habilitada. Para obter mais informações sobre como a Continuidade do Serviço pode usar o Cache de Host Local para manter o acesso do usuário a aplicativos e desktops durante interrupções de serviço, consulte Continuidade do serviço.

Como funciona

Durante operações normais, o Serviço de Provedor de Broker Remoto em um Cloud Connector se comunica com o Citrix Cloud para todas as operações de intermediação. O Serviço de Sincronização de Configuração Citrix (CSS) verifica regularmente as alterações de configuração no Citrix Cloud e sincroniza esses dados com o broker LHC no Cloud Connector. Se os Cloud

Connectors perderem a conectividade com o Citrix Cloud ou o Citrix Cloud estiver enfrentando um problema, o modo LHC é ativado e garante acesso contínuo a aplicativos e desktops.

Durante a operação normal de intermediação



- O Serviço de Provedor de Broker Remoto Citrix em um Cloud Connector aceita solicitações de conexão do StoreFront. O Serviço de Provedor de Broker Remoto se comunica com o Citrix Cloud para conectar usuários a VDAs que estão registrados no Citrix Cloud.
- O CSS verifica com o broker da nuvem no Citrix Cloud aproximadamente a cada 5 minutos para ver se alguma alteração de configuração foi feita. Essas alterações podem ser iniciadas pelo administrador (como alterar uma propriedade de grupo de entrega) ou ações do sistema (como atribuições de máquina).
- Se uma alteração de configuração ocorreu desde a verificação anterior, o CSS sincroniza as informações com o broker LHC no Cloud Connector. (O broker LHC também é conhecido como Serviço de Alta Disponibilidade, ou broker HA).

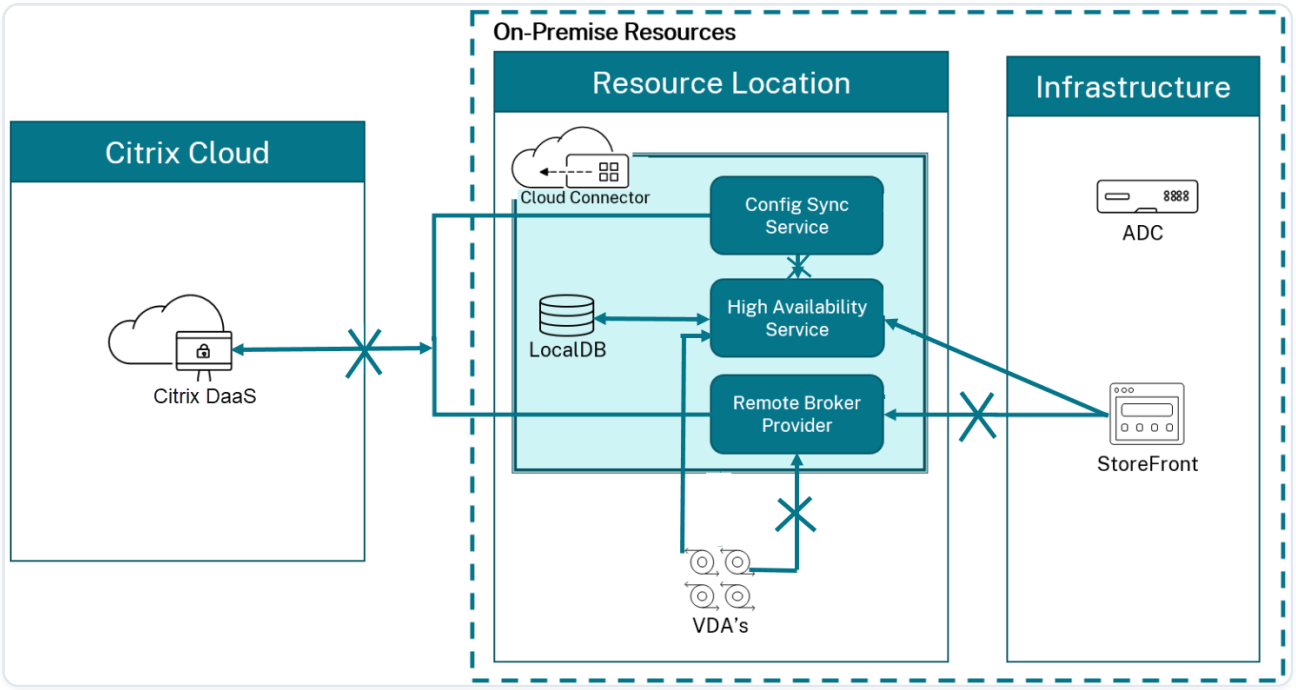
  Todos os dados de configuração são copiados, não apenas os itens que mudaram desde a verificação anterior. O CSS importa os dados de configuração para um banco de dados Microsoft SQL Server Express LocalDB no Cloud Connector. Este banco de dados é conhecido como banco de dados de Cache de Host Local. O CSS garante que as informações no banco de dados de Cache de Host Local correspondam às informações no banco de dados do site no Citrix Cloud.

  O Microsoft SQL Server Express LocalDB (usado pelo banco de dados LHC) é instalado automaticamente quando você instala um Cloud Connector. O banco de dados LHC não pode

ser compartilhado entre Cloud Connectors. Você não precisa fazer backup do banco de dados LHC. Ele é recriado toda vez que uma alteração de configuração é detectada.

- Se nenhuma alteração ocorreu desde a última verificação, os dados de configuração não são copiados.

Quando o modo LHC se torna ativo



- O broker LHC começa a escutar por informações de conexão e a processar solicitações de conexão.
- Quando os Cloud Connectors perdem a conectividade com o Citrix Cloud pela primeira vez, o broker LHC não possui dados de registro de VDA atuais, mas quando um VDA se comunica com ele, um processo de registro é acionado. Durante esse processo, o broker LHC também obtém informações de sessão atuais para esse VDA.
- Enquanto o broker LHC está lidando com as conexões, o Serviço de Provedor de Broker Remoto continua a monitorar a conexão com o Citrix Cloud. Quando a conexão é restaurada, o Serviço de Provedor de Broker Remoto instrui o broker LHC a parar de escutar por informações de conexão, e o Citrix Cloud retoma as operações de broker. Na próxima vez que um VDA se comunicar com o Citrix Cloud através do Serviço de Provedor de Broker Remoto, um processo de registro é acionado. O broker LHC remove quaisquer registros de VDA restantes de quando o modo LHC estava ativo. O CSS retoma a sincronização de informações quando descobre que ocorreram alterações de configuração no Citrix Cloud.

No caso improvável de o LHC iniciar durante uma sincronização, a importação atual é descartada e a última configuração conhecida é usada.

O log de eventos indica quando as sincronizações ocorrem e o modo LHC é ativado.

Não há limite de tempo imposto para operar no modo LHC.

Você também pode acionar manualmente o modo LHC. Consulte Forçar modo LHC para obter detalhes sobre por que e como fazer isso.

Zonas com vários Cloud Connectors

Entre outras tarefas, o CSS rotineiramente fornece ao broker LHC informações sobre todos os Cloud Connectors na zona. Com essas informações, cada broker LHC conhece todos os brokers LHC pares em execução em outros Cloud Connectors na zona.

Os brokers LHC se comunicam entre si em um canal separado. Esses brokers usam uma lista alfabética de nomes FQDN das máquinas em que estão sendo executados para determinar (eleger) qual broker LHC intermediará as operações na zona se a zona entrar no modo LHC. Durante o modo LHC, todos os VDAs se registram novamente com o broker LHC eleito. Os brokers LHC não eleitos na zona rejeitam ativamente as solicitações de conexão e registro de VDA de entrada.

> **Importante:**
>
> Conectores dentro de uma zona devem ser capazes de se comunicar entre si em `http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection`. Se os Conectores não puderem se comunicar neste endereço, vários brokers podem ser eleitos e falhas de inicialização ocorrerão quando no modo LHC.

> Durante o modo LHC, se um Cloud Connector for reiniciado ou o broker LHC falhar:

- Se esse Cloud Connector não for o broker LHC eleito, a reinicialização não terá impacto.
- Se esse Cloud Connector for o broker LHC eleito, o broker LHC no próximo Cloud Connector será eleito, fazendo com que os VDAs se registrem. A ordem de eleição é baseada na ordem alfabética do FQDN dos Cloud Connectors. Assim que o broker LHC se tornar ativo novamente, as operações LHC continuarão no primeiro conector em ordem alfabética, o que pode fazer com que os VDAs se registrem novamente. Neste cenário, o desempenho pode ser afetado durante os registros.

Consulte logs de eventos para obter mais informações sobre eventos relacionados às eleições de broker LHC.

Conteúdo dos dados do Cache de Host Local

O banco de dados LHC inclui os seguintes dados, que são um subconjunto dos dados no banco de dados principal:

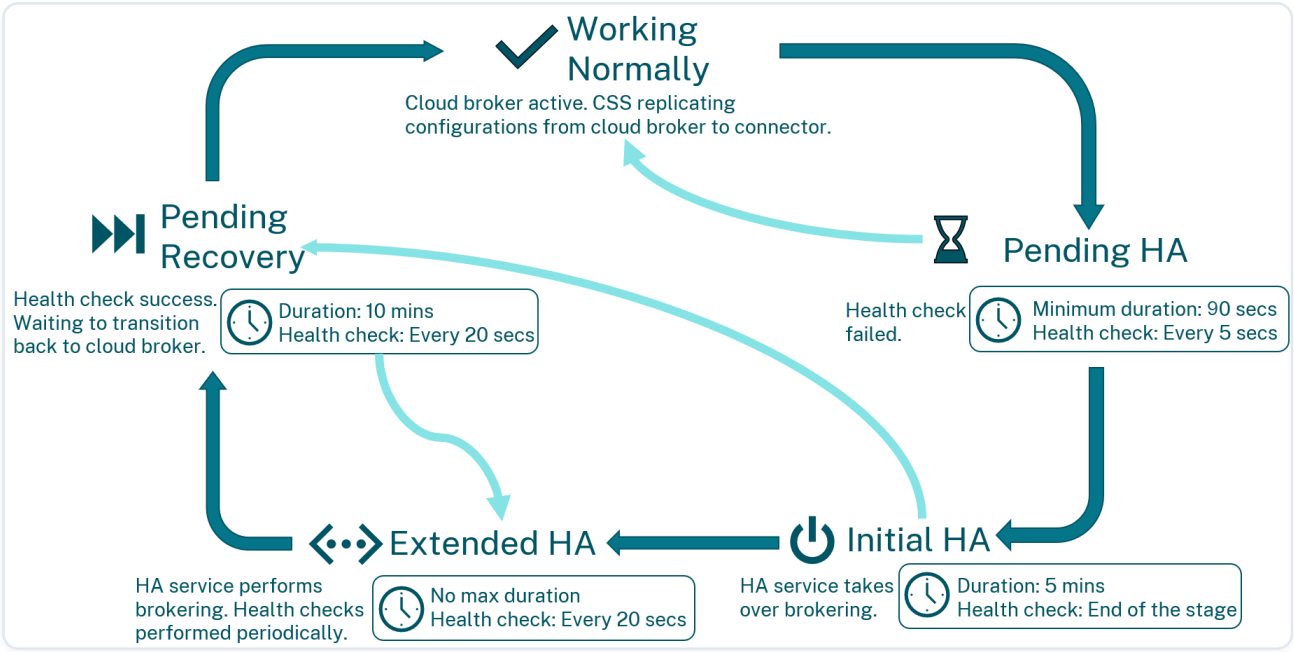
- Identidades de usuários e grupos que têm direitos atribuídos a recursos publicados do site.
- Identidades de usuários que estão usando atualmente, ou que usaram recentemente, recursos publicados do site.
- Identidades de máquinas VDA (incluindo máquinas de Acesso Remoto para PC) configuradas no site.
- Identidades (nomes e endereços IP) de máquinas cliente do aplicativo Citrix Workspace™ que estão sendo ativamente usadas para se conectar a recursos publicados.

Ele também contém as seguintes informações para conexões atualmente ativas que foram estabelecidas enquanto no modo LHC:

- Resultados de qualquer análise de endpoint de máquina cliente realizada pelo aplicativo Citrix Workspace.
- Identidades de máquinas de infraestrutura (como servidores Citrix Gateway e StoreFront) envolvidas com o site.
- Datas, horários e tipos de atividade recente por usuários

Estados do Cache de Host Local

Existem vários estados durante todo o ciclo de entrada e saída do modo LHC. O diagrama a seguir descreve os estados para entrar e sair do modo LHC.



- Durante o estado de **Funcionamento Normal**, todos os componentes estão saudáveis e todas as transações de corretagem são tratadas pelo broker da Nuvem. - - O CSS está replicando ativamente as configurações do broker da Nuvem para os Cloud Connectors. Se alguma verificação de integridade falhar, os Cloud Connectors fazem a transição para o estado **HA Pendente**. Nesse estado, uma verificação de integridade abrangente é iniciada para determinar o próximo curso de ação. Os conectores interagem com outros conectores na zona para determinar seu status de integridade.
- A decisão de passar de **HA Pendente** para **HA Inicial** é baseada no status de integridade de todos os conectores em uma determinada zona. Se as verificações de integridade forem bem-sucedidas, os conectores/controladores retornam ao estado de **Funcionamento Normal**. Alternativamente, se as verificações de integridade continuarem a falhar, os conectores/controladores fazem a transição para o estado **HA Inicial**.
- Durante o estado **HA Inicial**, o broker LHC no conector eleito assume as responsabilidades de corretagem. Todos os VDAs na zona atual que foram registrados anteriormente agora se registrarão com o broker LHC no Cloud Connector. Pode levar até 5 minutos para que todos os VDAs se registrem novamente com o Serviço HA. Ao final do **HA Inicial**, as verificações de integridade são iniciadas. Se todas as verificações de integridade forem bem-sucedidas, o estado faz a transição para **Recuperação Pendente**, caso contrário, o estado faz a transição para **HA Estendido**.
- As verificações de integridade continuam a ocorrer durante o período de **HA Estendido**. Quando as verificações de integridade são bem-sucedidas durante o **HA Estendido**, o estado faz a transição para **Recuperação Pendente**. Não há duração máxima de tempo para um conector permanecer no estado **HA Estendido**.
- **Recuperação Pendente** serve como um período de buffer para garantir que os serviços estejam totalmente saudáveis antes de fazer a transição para fora do modo LHC. Se alguma das verificações de integridade falhar durante a **Recuperação Pendente**, o estado faz a transição de volta para **HA Estendido**.
- Se todas as verificações de integridade forem bem-sucedidas durante todo o período de 10 minutos de **Recuperação Pendente**, o estado faz a transição para **Funcionamento Normal**. Com essa transição, o modo LHC termina, e todos os VDAs na zona que estavam registrados com o broker LHC agora se registram novamente com o broker da Nuvem. Esse novo registro pode levar novamente até 5 minutos.

Considerações importantes durante o modo LHC

Durante o modo LHC, considere os seguintes impactos:

ASPECTO	IMPACTO DURANTE O MODO LHC
Acesso ao Studio	Pode estar inacessível, dependendo da natureza da interrupção. Os VDAs em zonas operando no modo LHC são exibidos como **Não Registrados** no Studio porque estão registrados com o broker LHC.
Acesso Remoto ao SDK do PowerShell	Acesso limitado. Definir Autenticação do SDK: Execute `Get-XDAuthentication -ProfileName WindowsCurrentUser` para evitar que o proxy do SDK redirecione chamadas de cmdlet. Após fazer essas alterações, você pode usar todos os cmdlets `Get-Broker`. **Nota**: Inclua o parâmetro `-AdminAddress localhost:89` na chamada inicial do cmdlet. Exemplo: `Get-BrokerMachine -AdminAddress localhost:89`
Dados de Monitoramento	As funções de monitoramento não mostram atividade de quando o modo LHC está ativo. Um subconjunto de dados de

ASPECTO	IMPACTO DURANTE O MODO LHC
	monitoramento está disponível no painel de Cache de Host Local da página tendências no Monitor.
Credenciais do Hypervisor	Não podem ser obtidas do Serviço de Host. Máquinas em um estado de energia desconhecido, nenhuma operação de energia é possível. VMs ligadas são utilizáveis para conexões.
Máquinas Atribuídas	Utilizáveis apenas se atribuídas durante operações normais. Novas atribuições são impossíveis no modo LHC.
Máquinas de Acesso Remoto a PC	Inscrição e configuração automáticas não são suportadas. Máquinas inscritas e configuradas durante a operação normal são utilizáveis.
Limites de Sessão de Aplicativos e Desktops Hospedados em Servidor	Os usuários podem usar mais sessões do que seus limites de sessão configurados, se os recursos estiverem em zonas diferentes.
Comportamento da Zona	Cada zona age independentemente. Se o recurso verificação de integridade avançada do StoreFront estiver ativado, o StoreFront é capaz de rotear as solicitações de

ASPECTO	IMPACTO DURANTE O MODO LHC
	inicialização para a zona apropriada durante o modo LHC e evitar falhas na inicialização da sessão.
Reinicializações Agendadas de VDA	Se o modo LHC for ativado antes do início de uma reinicialização agendada para VDAs em um grupo de entrega, as reinicializações começarão quando o modo LHC for desativado e as operações normais de intermediação forem retomadas, potencialmente causando reinicializações inesperadas quando a zona sair do modo LHC. Para mais informações e configurações que podem alterar este comportamento, consulte Reinicializações agendadas atrasadas devido a interrupção do banco de dados.
Preferência de Zona	As configurações de preferência de zona não são consideradas para a inicialização da sessão.
Restrições de Tag	Para Grupos de Entrega com VDAs em várias zonas, as restrições de tag podem causar falhas de inicialização se os VDAs marcados não estiverem presentes em todas as zonas.

Nota:

O uso de `$XDSDKAuth` para autenticação SDK será descontinuado a partir de junho de 2025. Para detalhes, consulte Descontinuação.

Suporte a aplicativos e desktops

O LHC suporta os seguintes tipos de VDAs e modelos de entrega:

TIPO DE VDA	MODELO DE ENTREGA	DISPONIBILIDADE DE VDA DURANTE O MODO LHC
SO multissessão	Aplicativos e desktops	Sempre disponível.
SO de sessão única estático (atribuído)	Desktops	Sempre disponível.
SO de sessão única gerenciado por energia aleatório (agrupado)	Desktops	Disponível para apenas uma sessão por padrão. Você pode configurá-los para estarem sempre disponíveis para novas sessões durante o LHC. Para obter mais informações, consulte Habilitar usando o Studio e Habilitar usando o PowerShell. **Importante:** Habilitar o acesso a máquinas agrupadas de sessão única com

TIPO DE VDA	MODELO DE ENTREGA	DISPONIBILIDADE DE VDA DURANTE O MODO LHC	
		gerenciamento de energia pode fazer com que dados e alterações de sessões de usuário anteriores estejam presentes em sessões subsequentes.	

Nota:

Habilitar o acesso a VDAs de desktop com gerenciamento de energia em grupos de entrega agrupados não afeta como a propriedade `ShutdownDesktopsAfterUse` configurada funciona durante as operações normais. Quando o acesso a esses desktops durante o LHC é habilitado, os VDAs não reiniciam automaticamente após retornar às operações normais de intermediação. Os VDAs de desktop com gerenciamento de energia em grupos de entrega agrupados podem reter dados de sessões anteriores até que os VDAs reiniciem. Uma reinicialização do VDA pode ocorrer quando um usuário faz logoff do VDA durante operações sem LHC ou quando os administradores reiniciam o VDA.

Habilitar LHC para VDAs agrupados de SO de sessão única com gerenciamento de energia usando o Studio

Usando o Studio, você pode disponibilizar essas máquinas para novas conexões durante o modo LHC por grupo de entrega:

- Para habilitar esse recurso durante a criação do grupo de entrega, consulte Criar grupos de entrega.
- Para habilitar esse recurso para um grupo de entrega existente, consulte Gerenciar grupos de entrega

Nota:

> Essa configuração está disponível no Studio apenas para grupos de entrega de desktop agrupados que fornecem VDAs com gerenciamento de energia.

Habilitar LHC para VDAs agrupados de SO de sessão única com gerenciamento de energia usando o PowerShell

Para habilitar o LHC para VDAs em um grupo de entrega específico, siga estas etapas:

1. Habilite esse recurso no nível do site executando este comando:

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

2. Habilite o LHC para um grupo de entrega executando este comando com o nome do grupo de entrega especificado:

```
Set-BrokerDesktopGroup -Name "name"
-ReuseMachinesWithoutShutdownInOutage $true
```

Para alterar a disponibilidade padrão do LHC para grupos de entrega agrupados recém-criados com VDAs gerenciados por energia, execute o seguinte comando:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

> **Nota:**
>
> Alterar o padrão não altera a configuração para Grupos de Entrega existentes e afeta apenas os Grupos de Entrega criados usando o PowerShell.

Configuração do StoreFront

Se estiver usando uma implantação local do StoreFront, revise o seguinte:

- Se estiver usando um servidor virtual de balanceamento de carga, configure o servidor virtual para monitorar os Conectores com base nas capacidades de intermediação (por exemplo, use o monitor CITRIX-XD-DDC integrado em um NetScaler® para balanceamento de carga do conector).
- Inclua todos os Cloud Connectors dentro de um único locatário de nuvem como um único site no StoreFront.

- Visualize as configurações do NetScaler Gateway no StoreFront e certifique-se de que todos os Conectores estejam listados como servidores STA. Revise os dispositivos NetScaler e certifique-se de que todos os STAs listados no StoreFront estejam no mesmo formato no servidor virtual do NetScaler Gateway. A saúde do serviço STA também pode ser monitorada no servidor virtual do Gateway.
- Adicione todos os conectores ao feed de recursos no StoreFront e certifique-se de que o StoreFront possa se comunicar com todos os Cloud Connectors pela porta designada no feed de recursos.

> **Nota:**
>
> Para clientes com muitos conectores, pode ser benéfico configurar um servidor virtual de balanceamento de carga para cada zona para reduzir a sobrecarga de gerenciamento e simplificar a solução de problemas. Consulte Dicas da Citrix: Integrando o serviço Citrix Virtual Apps and Desktops e o StoreFront para obter mais informações.

Validar o funcionamento do Cache de Host Local

Para verificar se o LHC está configurado e funcionando corretamente:

- Certifique-se de que as importações de sincronização sejam concluídas com sucesso. Verifique os logs de eventos para obter mais informações sobre como monitorar as sincronizações do LHC.
- Certifique-se de que o banco de dados do Cache de Host Local foi criado em cada Cloud Connector. Isso confirma que o Serviço de Alta Disponibilidade pode assumir o controle, se necessário.
  - No servidor do Cloud Connector, navegue até `c:\Windows\ServiceProfiles\NetworkService`.
  - Verifique se `HaDatabaseName.mdf` e `HaDatabaseName_log.ldf` foram criados.
- Forçar modo LHC em todos os Cloud Connectors na zona: Depois de verificar que o Local Host Cache funciona, lembre-se de colocar todos os Cloud Connectors de volta ao modo normal. Consulte Estados do Local Host Cache para obter mais informações sobre o tempo que levará para sair do modo LHC.

Monitorar o Local Host Cache

Logs de eventos

Os logs de eventos fornecem informações críticas sobre a integridade e o desempenho do LHC.

Serviço de Sincronização de Configuração

Durante as operações normais, os seguintes eventos podem ocorrer quando o CSS importa os dados de configuração para o banco de dados LHC usando o broker LHC.

ID DO EVENTO	DESCRIÇÃO
503	Indica que o CSS recebeu uma configuração atualizada. Este evento ocorre cada vez que uma configuração atualizada é recebida do Citrix Cloud. Isso indica o início do processo de sincronização.
504	Indica que o CSS importou uma configuração atualizada. A importação da configuração foi concluída com êxito.
505	Indica que o CSS falhou em uma importação. A importação da configuração não foi concluída com êxito. Se uma configuração anterior bem-sucedida estiver disponível, ela será usada se o modo LHC for inserido. No entanto, estará desatualizada em relação à configuração atual. Se não houver nenhuma configuração anterior disponível, o serviço não poderá participar da intermediação de sessão durante o modo LHC. Neste caso, consulte a seção Solução de problemas e entre em contato com o Suporte Citrix.
507	Indica que o CSS abandonou uma importação porque o sistema está no modo LHC e o broker LHC está sendo usado para intermediação. O serviço recebeu uma nova configuração, mas a importação foi abandonada porque o modo LHC foi inserido. Este é um comportamento esperado.

ID DO EVENTO	DESCRIÇÃO
510	Indica que nenhum dado de configuração do CSS foi recebido do Serviço de Configuração primário.
517	Indica que houve um problema de comunicação com o Serviço de Broker primário.
518	Indica que o script CSS foi abortado porque o broker LHC (Serviço de Alta Disponibilidade) não está em execução.

Serviço de Alta Disponibilidade

Este serviço também é conhecido como o broker LHC.

ID DO EVENTO	DESCRIÇÃO
3502	Indica que ocorreu uma interrupção e o broker LHC está realizando operações de broker.
3503	Indica que uma interrupção foi resolvida e as operações normais foram retomadas.
3504	Indica o broker LHC eleito e outros brokers LHC envolvidos na eleição.
3507	Indica que o modo LHC está ativo no broker LHC eleito. Contém um resumo da interrupção, incluindo duração da interrupção, registro de VDA e informações da sessão.
3508	Indica que o LHC não está mais ativo no broker LHC eleito e as operações normais foram restauradas. Contém um resumo da interrupção, incluindo duração da interrupção, número de máquinas que se registraram durante o evento LHC e número de inicializações bem-sucedidas durante o modo LHC.

ID DO EVENTO	DESCRIÇÃO
3509	Indica que o LHC está ativo no broker LHC não eleito. Contém uma duração de interrupção a cada 2 minutos e indica o broker LHC eleito.
3510	Indica que o LHC não está mais ativo no broker LHC não eleito. Contém a duração da interrupção e indica o broker LHC eleito.

Provedor de Broker Remoto

Este serviço atua como um proxy entre o Citrix Cloud e seus VDAs e Cloud Connectors.

ID DO EVENTO	DESCRIÇÃO
3001	A primeira detecção de uma falha que faz com que o Cloud Connector entre no estado **HA Pendente**. As verificações de integridade começam a avaliar se a falha é transitória ou persistente. Após o tempo alocado no estado **HA Pendente**, os resultados mais recentes da verificação de integridade indicam se é necessária uma entrada no modo LHC ou se as operações normais podem ser retomadas.
3002	Indica que o Cloud Connector não pode entrar no modo LHC. O motivo está incluído nas informações do evento.
3003	Indica que o Cloud Connector está em transição pelos estados do modo LHC. O evento

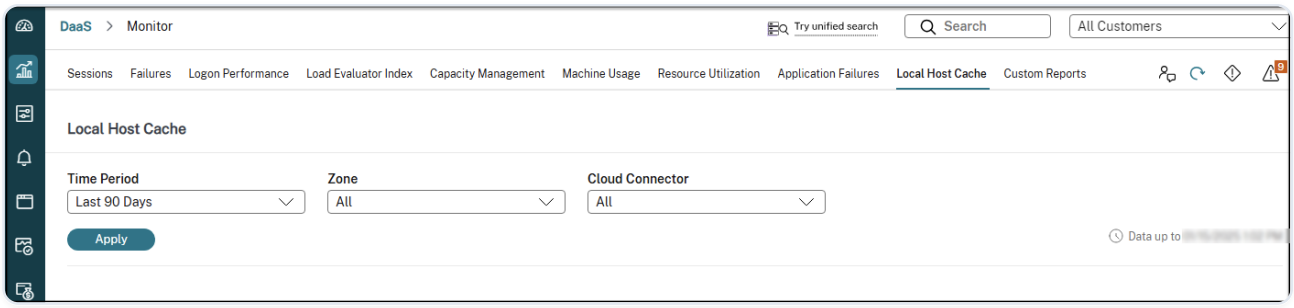
ID DO EVENTO	DESCRIÇÃO	
	fornece detalhes sobre o seguinte • estado do qual o Cloud Connector está em transição • estado para o qual está em transição • duração do estado anterior	

Nota:

Os eventos **3001** em seus Cloud Connectors periodicamente ao longo do dia geralmente não são motivo de preocupação. No entanto, se estiverem ocorrendo várias vezes por hora, isso indica um problema de rede e pode justificar uma investigação mais aprofundada.

Citrix Monitor

O Citrix Monitor contém informações centralizadas sobre entradas do modo LHC e desempenho para as diferentes Zonas em seu ambiente.



Consulte Monitorar tendências históricas em um site para obter mais informações.

Forçar o modo Local Host Cache

Você pode querer forçar deliberadamente o modo Local Host Cache nos seguintes cenários:

- Se sua rede estiver caindo e voltando repetidamente: Forçar o LHC até que os problemas de rede sejam resolvidos evita a transição contínua entre os modos normal e LHC (e as frequentes tempestades de registro de VDA resultantes).
- Para testar um plano de recuperação de desastres.
- Para ajudar a garantir que o Local Host Cache esteja funcionando corretamente.

Para forçar o modo LHC:

1. Edite o registro de cada servidor Cloud Connector em `HKLM\Software\Citrix\DesktopServer\LHC`: Crie e defina `OutageModeForced` como REG_DWORD para `1`.
    - Definir o valor como `1` instrui o broker LHC a entrar no modo LHC, independentemente do estado da conexão com o Citrix Cloud.
    - Definir o valor como `0` instrui o broker LHC a sair do modo LHC e retomar as operações normais.

Para verificar eventos:

1. Monitore o arquivo de log `Current_HighAvailabilityService` em `C:\ProgramData\Citrix\workspaceCloud\Logs\Plugins\HighAvailabilityService`.

Solucionar falhas de importação de sincronização

Quando uma importação de sincronização para o banco de dados LHC falha e um evento 505 é registrado, você pode usar as seguintes ferramentas de solução de problemas:

- Rastreamento CDF:
    - Habilite o rastreamento para os módulos `ConfigSyncServer` e `BrokerLHC`.
    - Use com outros módulos de broker para identificar o problema.
- Relatório de Rastreamento CSS:
    - Gera um relatório detalhado que identifica o objeto que causa a falha de sincronização.

> **Nota:**
>
> A habilitação deste relatório pode afetar a velocidade da sincronização. Desative-o quando não estiver solucionando problemas ativamente.

Para habilitar e gerar um Relatório de Rastreamento CSS:

a. Habilitar relatórios: Execute o seguinte comando:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

b. Localize o relatório: O relatório HTML é gerado em `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncRepo`

c. Desabilitar relatórios: Após a geração do relatório, execute o seguinte comando para desabilitar o recurso de relatórios:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

Comandos PowerShell do Cache de Host Local

Você pode gerenciar o Cache de Host Local em seus Cloud Connectors usando comandos PowerShell.

O módulo PowerShell está no seguinte local nos Cloud Connectors:

`C:\Program Files\Citrix\Broker\Service\ControlScripts`

> **Importante:**
>
> Execute este módulo apenas nos Cloud Connectors.

Importar módulo PowerShell

Para importar o módulo, execute o seguinte no seu Cloud Connector:

```
Import-Module "C:\Program
Files\Citrix\Broker\Service\ControlScripts\HighAvailabilityServiceControl.
psm1
```

Comandos PowerShell para gerenciar o LHC

Os seguintes cmdlets ajudam você a ativar e gerenciar o modo LHC nos Cloud Connectors.

CMDLETS	FUNÇÃO
`Enable-LhcForcedOutageMode`	Coloca o Broker no modo LHC. Os arquivos de banco de dados do Local Host Cache devem ter sido criados com sucesso pelo CSS para que `Enable-LhcForcedOutageMode` funcione corretamente. Este cmdlet apenas força o LHC no Cloud Connector onde foi executado. Para que o LHC se torne ativo, este cmdlet deve ser executado em todos os Cloud Connectors dentro da zona.
`Disable-LhcForcedOutageMode`	Tira o Broker do modo LHC. Este cmdlet apenas desativa o modo LHC no Cloud Connector onde foi executado. `Disable-LhcForcedOutageMode` deve ser executado em todos os Cloud Connectors dentro da zona.
`Set-LhcConfigSyncIntervalOverride`	Define o intervalo no qual o CSS verifica alterações de configuração no site do Citrix DaaS™. O intervalo de tempo pode variar de 60 segundos (um minuto) a 3600 segundos (uma hora). Essa configuração se aplica apenas ao Cloud Connector no qual foi executada. Para consistência entre os Cloud Connectors, considere executar este cmdlet em cada Cloud Connector. Por exemplo: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Define o intervalo no qual o CSS verifica alterações de configuração no site do Citrix DaaS para o valor padrão de 300 segundos (cinco minutos). Essa configuração se aplica apenas ao Cloud Connector no qual foi executada. Para consistência entre os Cloud Connectors, considere executar este cmdlet em cada Cloud Connector.

CMDLETS	FUNÇÃO
`Enable-LhcHighAvailabilitySDK`	Habilita o acesso a todos os cmdlets `Get-Broker*` dentro do Cloud Connector no qual foi executado.
`Disable-LhcHighAvailabilitySDK`	Desabilita o acesso aos comandos do Broker PowerShell dentro do Cloud Connector no qual foi executado.

Nota:

- Use a porta 89 ao executar os cmdlets `Get-Broker*` no Cloud Connector. Por exemplo:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- Quando não está no modo LHC, o Broker LHC no Cloud Connector contém apenas informações de configuração.
- Durante o modo LHC, o Broker LHC contém as seguintes informações:
  - Estados dos recursos
  - Detalhes da sessão
  - Registros de VDA
  - Informações de configuração

Mais informações

- Consulte Considerações de escala e tamanho para o Cache de Host Local para obter informações sobre:
  - Metodologias e resultados de teste
  - Considerações sobre o tamanho da RAM
  - Considerações sobre a configuração de núcleos de CPU e soquetes
  - Considerações sobre armazenamento
- Resumo Técnico: Cache de Host Local

    - Evite configurações incorretas comuns que podem impactar negativamente a resiliência do DaaS

- A ferramenta de visibilidade em tempo real do Cache de Host Local (LHC) é uma solução abrangente baseada em PowerShell para fornecer visibilidade em ambientes de Cache de Host Local da Citrix. Ela oferece interfaces de linha de comando e GUI simples acessíveis a partir do Cloud Connector para que você possa:

    - Descobrir Cloud Connectors em uma zona ou local de recurso
    - Identificar o líder eleito durante o modo LHC
    - Habilitar ou desabilitar o modo de interrupção forçada em todos os Cloud Connectors na zona ou local de recurso
    - Consultar logs de eventos de provedores específicos e IDs de Evento
    - Executar comandos Broker PowerShell no líder eleito

    Para obter mais informações, consulte Ferramenta de Visibilidade do Cache de Host Local.

Ferramenta de Visibilidade do Cache de Host Local

Este artigo descreve a Ferramenta de Visibilidade em Tempo Real do Cache de Host Local (LHC), uma solução baseada em PowerShell que fornece visibilidade em ambientes de Cache de Host Local da Citrix. Usando esta ferramenta, você pode monitorar a saúde do Cloud Connector, identificar o líder eleito durante o modo LHC, controlar o modo de interrupção forçada e consultar logs de eventos para solucionar problemas de comportamento do LHC.

Visão geral

A Ferramenta de Visibilidade em Tempo Real do Cache de Host Local (LHC) é uma solução abrangente baseada em PowerShell para fornecer visibilidade em ambientes de Cache de Host Local da Citrix. Ela oferece uma interface de linha de comando e GUIs simples acessíveis a partir do Cloud Connector para que você possa:

- Descobrir Cloud Connectors em uma zona ou local de recurso.
- Identificar o líder eleito durante o modo LHC.
- Habilitar ou desabilitar o modo de interrupção forçada em todos os Cloud Connectors na zona ou local de recurso.
- Consultar logs de eventos de provedores e IDs de Evento específicos.
- Executar comandos Broker PowerShell no líder eleito.

Pré-requisitos

Antes de implantar e executar a Ferramenta de Visibilidade do Cache de Host Local, certifique-se de que seu ambiente atenda aos seguintes requisitos de sistema, permissões e arquivos.

Requisitos do sistema

- Windows Server 2016 ou posterior
- PowerShell 5.1 ou superior
- Deve ser executado em um Citrix Cloud Connector™
- Serviços necessários:
  - Serviço de Alta Disponibilidade Citrix
  - Serviço ConfigSync Citrix

Permissões

- Privilégios de administrador na máquina local
- Permissões de execução remota do PowerShell para todos os Cloud Connectors na zona
- Conectividade de rede para todos os Cloud Connectors

Arquivos necessários

- `LHCVisibilityTool.ps1` - Módulo principal do PowerShell
- `LHCVisibilityToolGUI.ps1` - Aplicativo GUI
- `HighAvailabilityServiceControl.psm1` - Módulo de Controle do Serviço HA Citrix

O script PowerShell da GUI está localizado em:

```
C:\Program Files\Citrix\Broker\Service\LHCVisibilityToolScripts
```

Introdução

Antes de executar a ferramenta, defina a política de execução do PowerShell usando uma das seguintes opções:

- Opção 1: RemoteSigned (mais restritiva):

  ```
  Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
  ```

- Opção 2: Somente sessão atual (temporário):

```
Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process
```

Nota:

Pode ser necessário executar o PowerShell como Administrador para alterar a política de execução. Se você tiver apenas permissões de nível de usuário, use `-Scope CurrentUser`.

Use a ferramenta por meio do aplicativo GUI

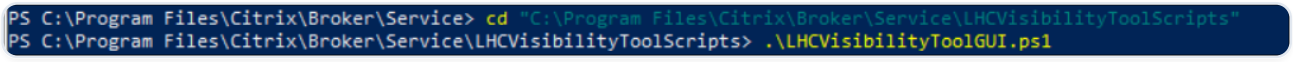
A GUI fornece uma interface com guias para descobrir Cloud Connectors, controlar o modo de interrupção, consultar logs de eventos e executar comandos de broker. Depois de iniciar a ferramenta, selecione uma tarefa para ir às suas instruções:

- Iniciar a GUI
- Descobrir Cloud Connectors e identificar o líder
- Controlar o modo de interrupção forçada
- Consultar e rastrear logs de eventos
- Executar comandos de broker
- Visualizar logs de sessão

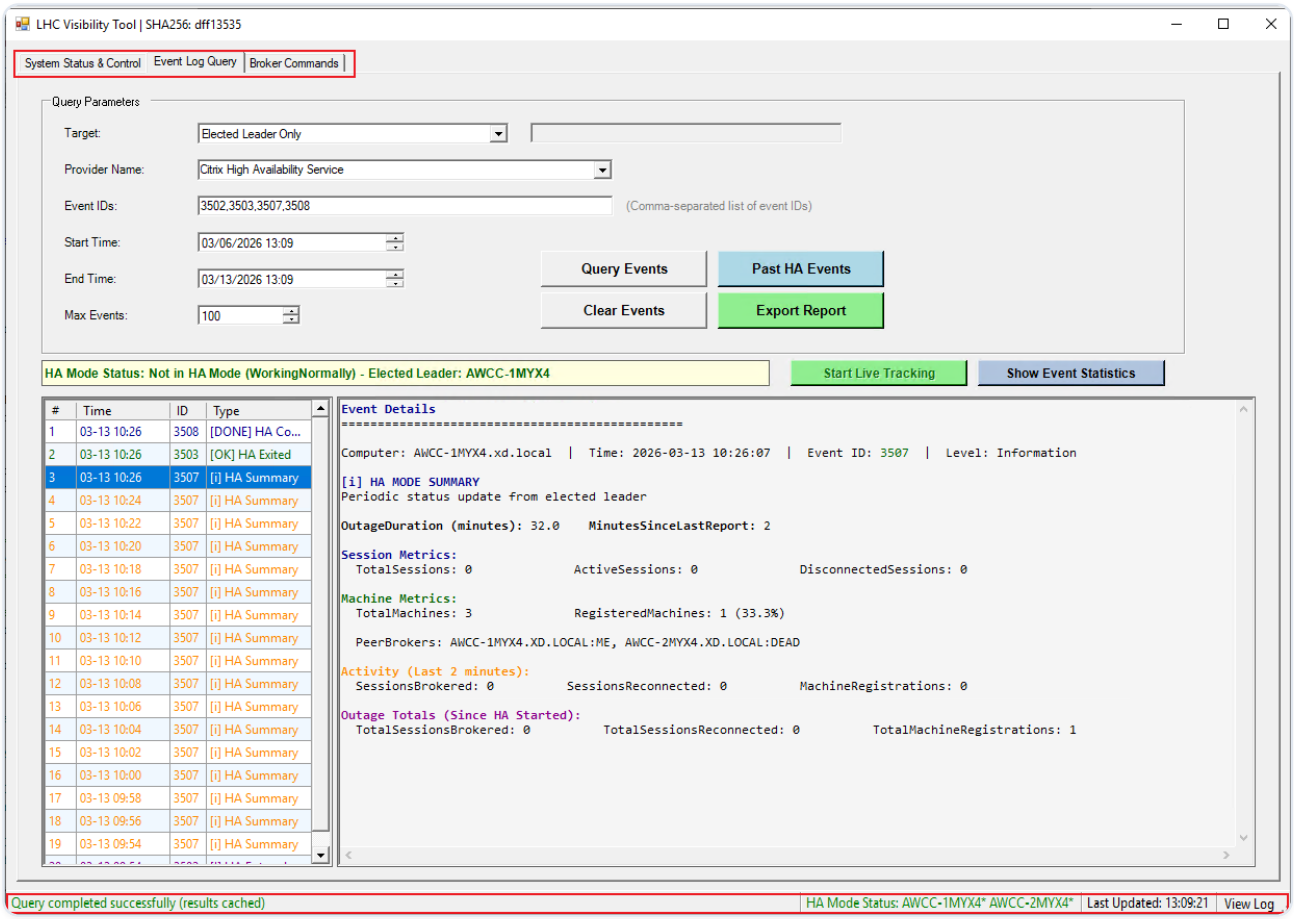
INICIAR A GUI

```
cd "C:\Program Files\Citrix\Broker\Service\LHCVisibilityToolScripts"

.\LHCVisibilityToolGUI.ps1
```



A ferramenta usa um layout de três guias com uma barra de status persistente na parte inferior.



A barra de status se estende pela parte inferior da janela e contém:

ITEM	DESCRIÇÃO
Status da operação (esquerda)	Operação atual, ou "Pronto"
Status do Modo HA	Indicadores de ponto por conector (máximo de 5 mostrados; "+N mais" se truncado); a dica de ferramenta ao passar o mouse mostra a lista completa
Última Atualização	Carimbo de data/hora da última atualização bem-sucedida do estado HA
Visualizar Log	Abre o arquivo de log da sessão no Bloco de Notas

A barra de status usa as seguintes cores para indicar o estado HA:

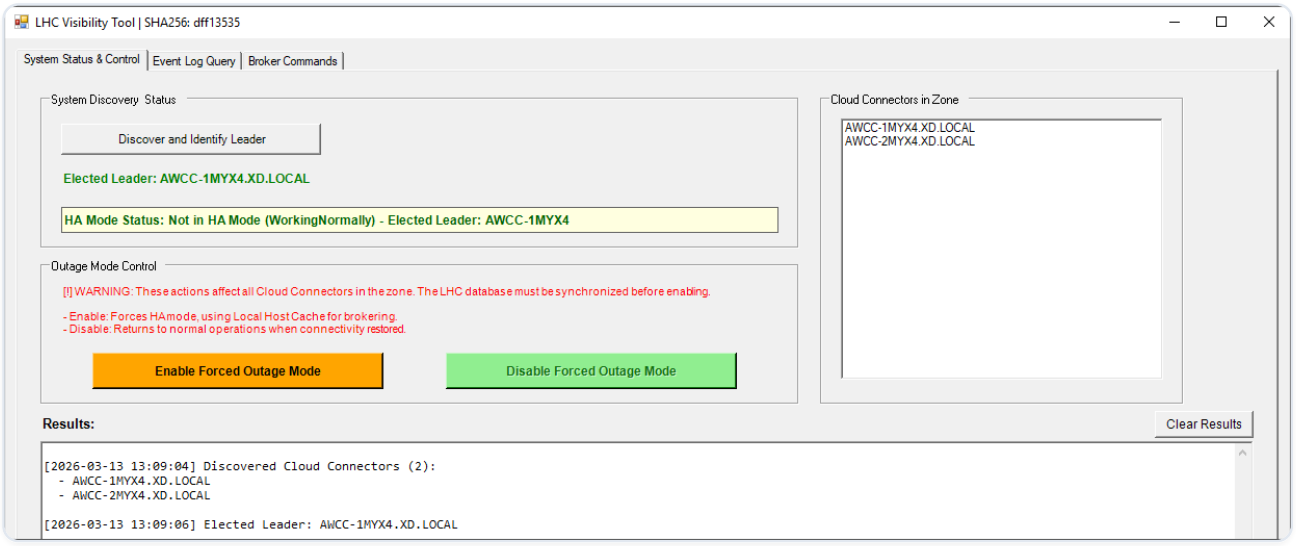
ESTADO	COR
FuncionandoNormalmente	Verde

ESTADO	COR
HA Pendente	Dourado
Recuperação Pendente	Laranja
HA Inicial	Vermelho
HA Estendido	Vermelho
Desconhecido / Inacessível	Cinza

DESCOBRIR CLOUD CONNECTORS E IDENTIFICAR O LÍDER

Na guia **Status e Controle do Sistema**, clique em **Descobrir e Identificar Líder**. A ferramenta detecta e mostra automaticamente o líder eleito entre todos os Cloud Connectors na zona usando:

- Análise de log de eventos (ID de Evento 3504)
- Informações de PeerStatus e IsElected do Registro
- Verificação de serviço local



CONTROLAR O MODO DE INTERRUPÇÃO FORÇADA

Na guia **Status e Controle do Sistema**, use os controles do modo de interrupção para gerenciar o modo HA em toda a zona:

- **Habilitar Modo de Interrupção Forçada:**
  - Força todos os Cloud Connectors na zona a entrar no modo HA
  - Usa o Cache de Host Local para o gerenciamento de conexões

    - Requer que o banco de dados LHC seja sincronizado

- **Desabilitar Modo de Interrupção Forçada:**
    - Permite que o sistema retorne às operações normais
    - Reconecta-se ao site principal quando disponível

> **Aviso:**
>
> Essas ações afetam todos os Cloud Connectors na zona.

CONSULTAR E RASTREAR LOGS DE EVENTOS

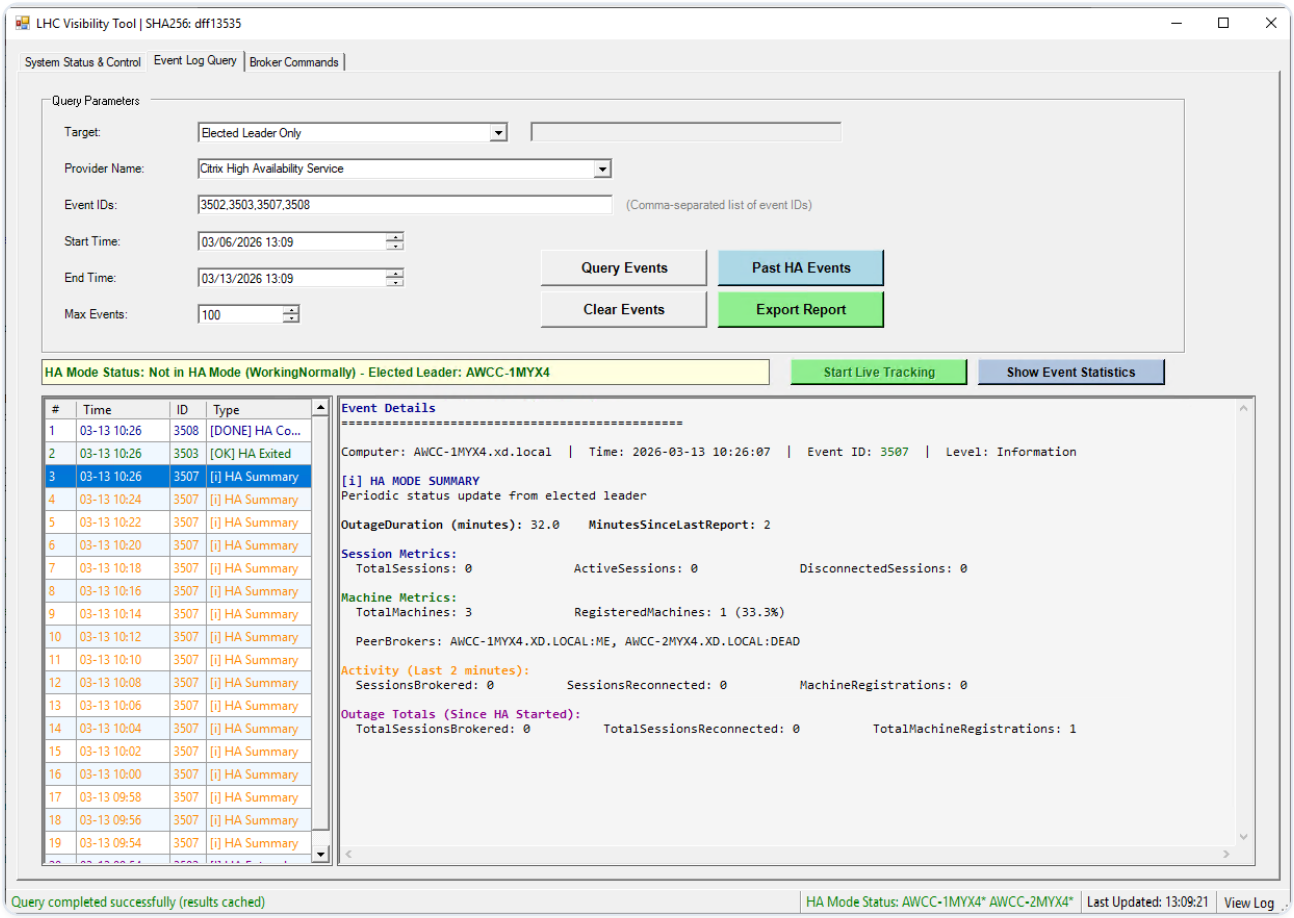
Na guia **Consulta de Log de Eventos**, configure os seguintes parâmetros de consulta:

- **Alvo:** Escolha entre:
    - Todos os Cloud Connectors
    - Somente Líder Eleito
    - Computador Específico (insira o FQDN)
- **Nome do Provedor:** Selecione ou insira um provedor personalizado:
    - Serviço de Alta Disponibilidade Citrix
    - Serviço Citrix ConfigSync
    - Serviço Citrix Broker
- **IDs de Evento:** Lista separada por vírgulas (por exemplo, `3502,3503,3506`)
- **Intervalo de Tempo:** Opcionalmente, filtre por hora de início e fim
- **Eventos Máximos:** Número máximo de eventos a serem recuperados por computador (padrão: 100)

Use os seguintes botões para trabalhar com eventos:

- **Consultar Eventos:** Consulta os logs de eventos usando os parâmetros de consulta configurados.
- **Eventos HA Anteriores:** Encontra os limites de início e fim do LHC (eventos 3502, 3503, 3508) a partir dos parâmetros de consulta configurados e exibe o evento de resumo final para fornecer uma visão geral.

- **Limpar Eventos:** Limpa a lista de eventos, o painel de detalhes e o estado de rastreamento.
- **Export Report:** Cria estatísticas a partir dos eventos consultados na GUI e as salva como um arquivo de texto. (Usa a saída do botão **Show Event Statistics**.)



O rastreamento em tempo real funciona da seguinte forma:

- O rastreamento em tempo real monitora novos eventos de resumo a cada 120 segundos enquanto o LHC estiver ativo.
- Quando o rastreamento em tempo real começa, ele determina o horário de início para o modo LHC referenciando o evento 3502 e lista todos os eventos que apareceram desde o início.
- O rastreamento em tempo real pode ser interrompido manualmente ou automaticamente quando o modo LHC é concluído.

A seção inferior fornece duas visualizações principais:

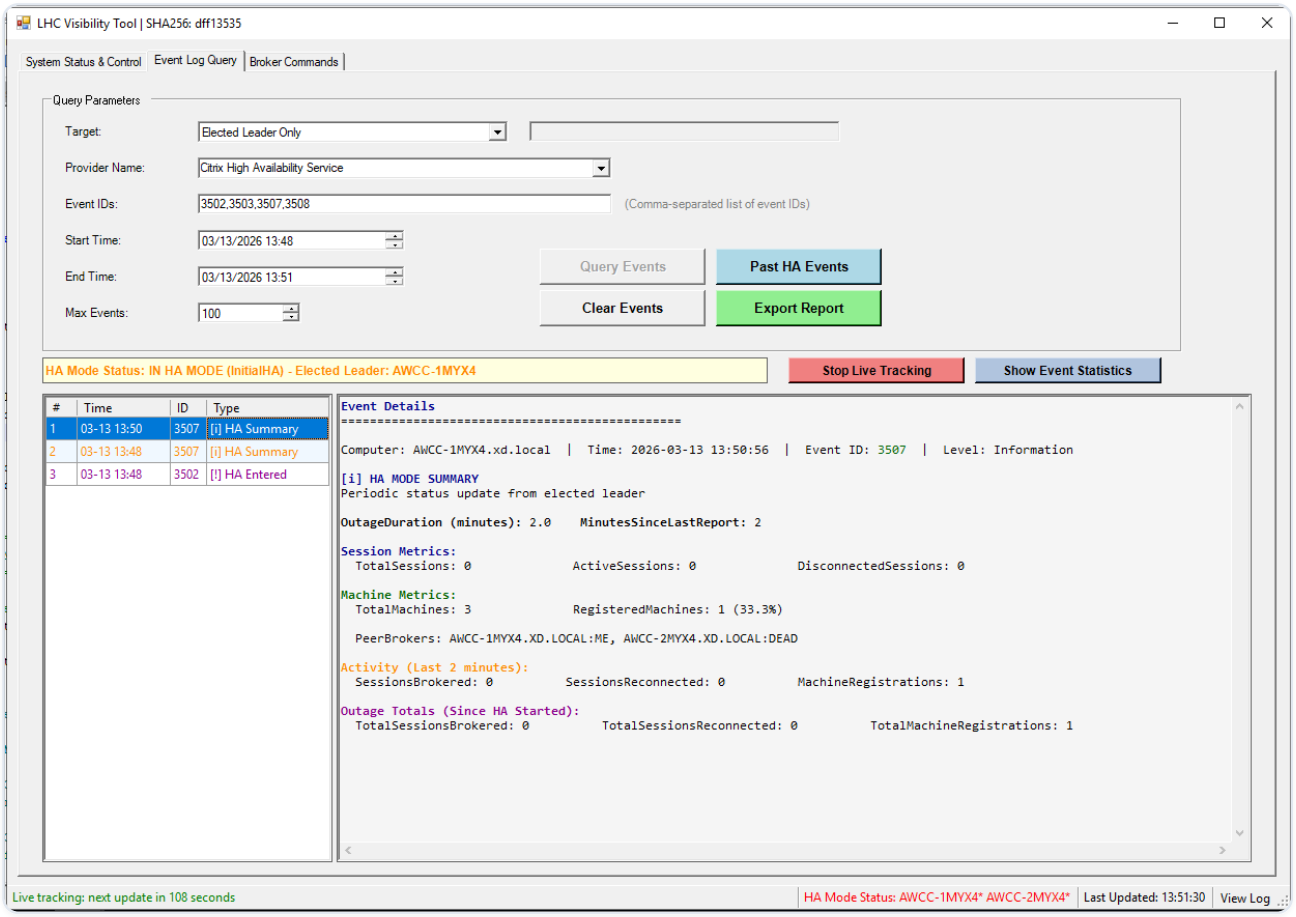
- **Painel esquerdo:**
  - Os eventos são listados cronologicamente com detalhes importantes (número do evento, hora, ID, tipo).
  - Cada evento é visualmente distinguido por cor com base em seu tipo, seguindo a referência do ID do evento.

    - A seleção de um evento exibe mais informações sobre ele.

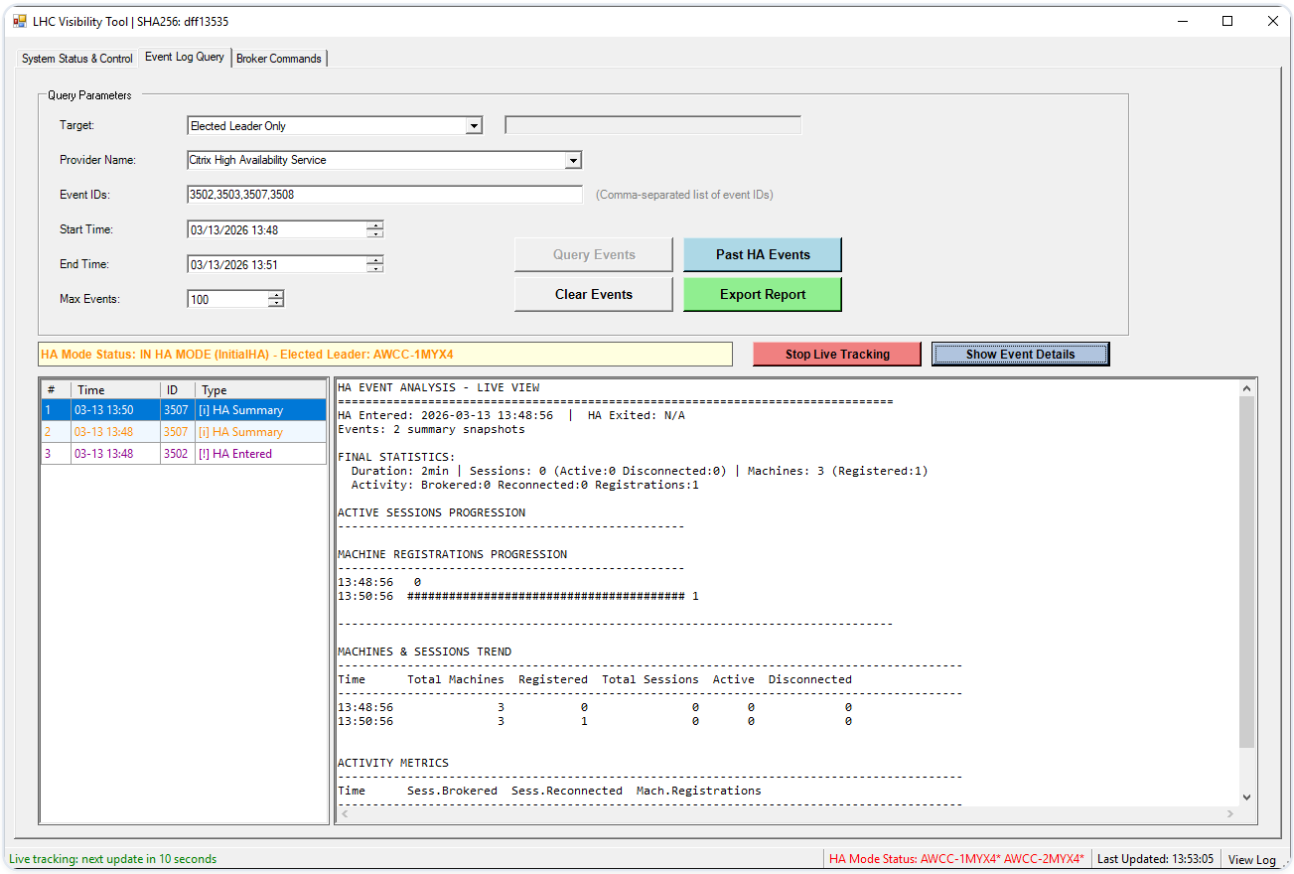
- **Painel direito:** Duas opções de exibição permitem alternar entre resumos estatísticos e informações detalhadas para o evento selecionado:

    - **Show Event Details:** Detalhes abrangentes para o evento escolhido.
    - **Show Event Statistics:** Estatísticas que resumem os eventos do modo HA, incluindo métricas tabulares e gráficos de barras ASCII de eventos de resumo (3507).

A imagem a seguir mostra a visualização de detalhes do evento:



A imagem a seguir mostra a visualização de estatísticas de eventos:



Referência: IDs de evento de HA e ConfigSync

As seções a seguir listam IDs de Evento comuns por provedor.

Serviço de Alta Disponibilidade Citrix:

ID DO EVENTO	DESCRIÇÃO
3502	Modo HA ativado (broker eleito)
3503	Fora do modo HA (operações normais retomadas)
3506	Modo HA ativado (broker não eleito)
3507	Resumo periódico do modo HA (broker eleito)
3508	Fim do resumo do modo HA (broker eleito)

Serviço Citrix ConfigSync:

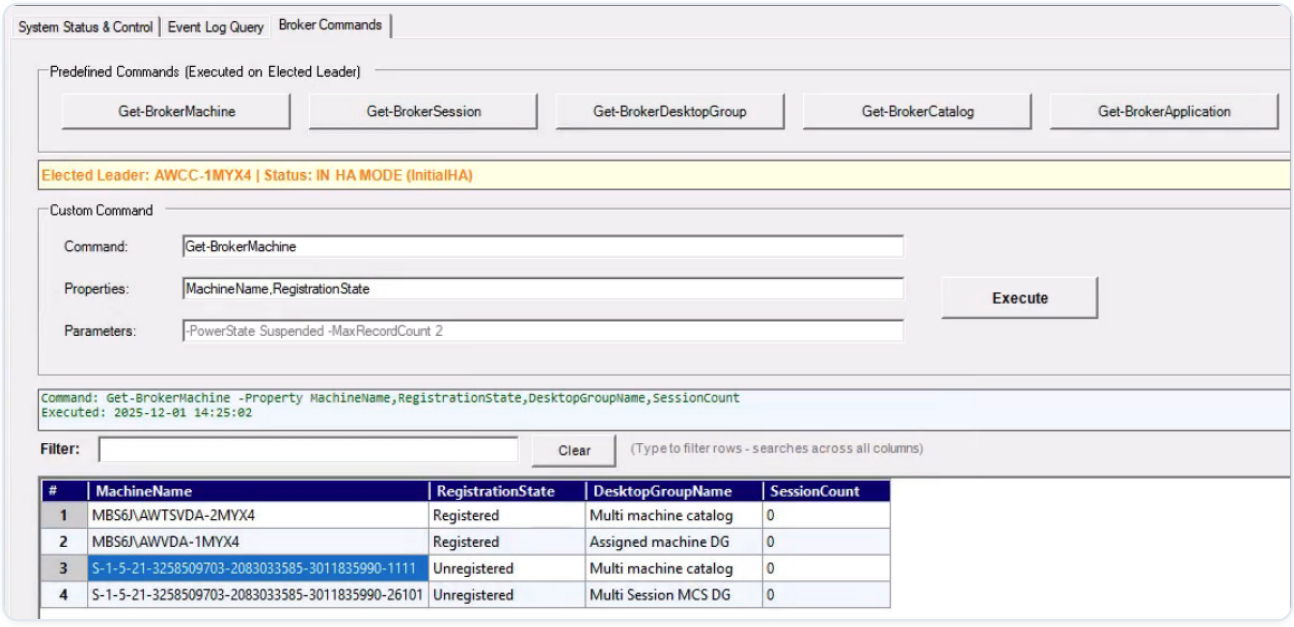
ID DO EVENTO	DESCRIÇÃO
503	Processo de sincronização iniciado

ID DO EVENTO	DESCRIÇÃO
504	Sincronização concluída com sucesso
505	Sincronização falhou
507	Sincronização abandonada devido ao modo HA
510	Nenhum dado de configuração recebido
517	Problema de comunicação com o broker primário
518	ConfigSync abortado (Serviço HA não em execução)

EXECUTAR COMANDOS DO BROKER

Na guia **Comandos do Broker**, os comandos predefinidos são:

- **Get-BrokerMachine:** Recuperar informações de VDA/máquina
- **Get-BrokerSession:** Recuperar sessões ativas
- **Get-BrokerDesktopGroup:** Recuperar grupos de entrega
- **Get-BrokerCatalog:** Recuperar catálogos de máquinas
- **Get-BrokerApplication:** Recuperar aplicativos publicados

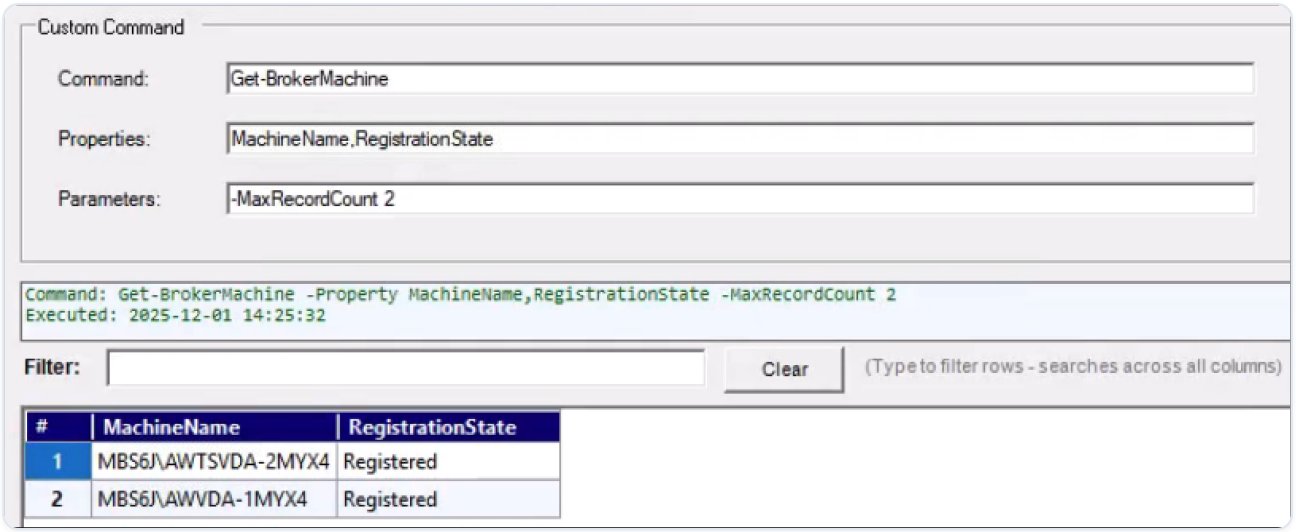


> **Dica:**

> Use a caixa de texto do filtro para pesquisar simultaneamente em todas as colunas de string por um item específico nos resultados.

> Para executar um comando personalizado:

1. Insira um comando, por exemplo `Get-BrokerMachine -MaxRecordCount 2`.
2. Opcionalmente, especifique as propriedades a serem retornadas (separadas por vírgulas).
3. Clique em **Executar**.



> **Nota:**

> Os comandos do Broker fornecem informações recentes do banco de dados LHC quando:

> - O sistema está no modo LHC.
> - Um líder eleito foi identificado.
> - O banco de dados LHC está disponível.

VISUALIZAR LOGS DE SESSÃO

Para abrir o log da sessão atual, clique em **Visualizar Log** na barra de status. O log é aberto no Bloco de Notas.

Cada sessão cria um arquivo de log em `%TEMP%\LHCVisibilityTool_<yyyyMMdd_HHmmss>.log`. As mensagens também são gravadas no console do host com codificação de cores.

Usar a ferramenta via linha de comando

Além da GUI, você pode executar a ferramenta diretamente do PowerShell. Depois de importar o módulo, use os seguintes comandos para executar cada tarefa. Selecione uma tarefa para ir ao seu comando:

- Iniciar a ferramenta de linha de comando
- Descobrir Cloud Connectors
- Identificar o líder eleito
- Obter o estado de interrupção
- Consultar logs de eventos
- Executar comandos do broker
- Controlar o modo de interrupção

INICIAR A FERRAMENTA DE LINHA DE COMANDO

```
cd "C:\Program Files\Citrix\Broker\Service\LHCVisibilityToolScripts"

. .\LHCVisibilityTool.ps1
```

DESCOBRIR CLOUD CONNECTORS

```
$connectors = Get-CloudConnectorsInZone

$connectors | ForEach-Object { Write-Host $_ }
```

IDENTIFICAR O LÍDER ELEITO

```
$leader = Get-ElectedLeader

Write-Host "Elected Leader: $leader"
```

OBTER O ESTADO DE INTERRUPÇÃO

```
$states = Get-OutageState

foreach ($connector in $states.Keys) {
```

```
    Write-Host "$connector : $($states[$connector].State)"

}
```

CONSULTAR LOGS DE EVENTOS

Consultar todos os Cloud Connectors para eventos de HA:

```
$results = Get-LHCEventLogs -EventID @(3502, 3503, 3506) `

    -ProviderName "Citrix High Availability Service" `

    -StartTime (Get-Date).AddDays(-7) `

    -EndTime (Get-Date) `

    -MaxEvents 100



# Display results

foreach ($computer in $results.Keys) {

    Write-Host "`n=== $computer ==="

    if ($results[$computer].Success) {

        $results[$computer].Events | Format-Table TimeCreated, Id, Message
-AutoSize

    } else {

        Write-Host "ERROR: $($results[$computer].Error)" -ForegroundColor
Red

    }

}
```

Consultar apenas o líder eleito:

```
$results = Get-LHCEventLogs -ComputerName "ElectedLeader" `
    -EventID @(3507) `
    -ProviderName "Citrix High Availability Service" `
    -MaxEvents 50
```

Consultar um computador específico:

```
$results = Get-LHCEventLogs -ComputerName "CC-01.domain.com" `
    -EventID @(503, 504, 505) `
    -ProviderName "Citrix ConfigSync Service"
```

EXECUTAR COMANDOS DO BROKER

Obter todas as máquinas:

```
$machines = Invoke-BrokerCommand -Command "Get-BrokerMachine" `
    -Properties @("MachineName", "RegistrationState", "SessionCount")
$machines | Format-Table -AutoSize
```

Obter sessões ativas:

```
$sessions = Invoke-BrokerCommand -Command "Get-BrokerSession" `
    -Properties @("UserName", "MachineName", "SessionState")
$sessions | Format-Table -AutoSize
```

Executar um comando personalizado com parâmetros:

```
$params = @{
    MaxRecordCount = 10
}
```

```
$results = Invoke-BrokerCommand -Command "Get-BrokerMachine" `

    -Parameters $params `

    -Properties @("MachineName", "DesktopGroupName")
```

CONTROLAR O MODO DE INTERRUPÇÃO

Habilitar o modo de interrupção forçada em todos os Cloud Connectors:

```
$results = Set-LHCOutageMode -Enable



# Check results

foreach ($connector in $results.Keys) {

    $status = if ($results[$connector].Success) { "SUCCESS" } else
{ "FAILED" }

    Write-Host "$connector : $status"

    if (-not $results[$connector].Success) {

        Write-Host "  Error: $($results[$connector].Error)"
-ForegroundColor Red

    }

}
```

Desabilitar o modo de interrupção forçada:

```
$results = Set-LHCOutageMode



# Check results

foreach ($connector in $results.Keys) {
```

```
    $status = if ($results[$connector].Success) { "SUCCESS" } else
{ "FAILED" }

    Write-Host "$connector : $status"

}
```

Solução de problemas

Para solucionar problemas com a ferramenta, siga este processo geral:

1. Verifique o log de eventos do aplicativo para mensagens de erro detalhadas.
2. Verifique se todos os pré-requisitos foram atendidos.
3. Revise os problemas comuns na tabela a seguir e as melhores práticas descritas posteriormente neste artigo.
4. Consulte Cache de Host Local e o resumo técnico Evite Configurações Incorretas Comuns que Podem Impactar Negativamente a Resiliência do DaaS.

A tabela a seguir lista problemas comuns que você pode encontrar ao usar a ferramenta e suas soluções recomendadas.

PROBLEMA	SOLUÇÃO
Nenhum Cloud Connector encontrado	1. Verifique se você está executando em um Cloud Connector. 2. Verifique se os serviços necessários estão em execução usando `Get-Service CitrixHighAvailabilityService, CitrixConfigSyncService`. 3. Verifique a chave de registro `HKLM:\SOFTWARE\Citrix\Bro`

PROBLEMA	SOLUÇÃO
	`ker\Service\State\LHC`.
Não é possível identificar o líder eleito	1. Verifique o ID do Evento 3502 no log de Aplicativos. 2. Verifique a conectividade com todos os Cloud Connectors.
Comando do Broker falhou	1. Certifique-se de que o sistema esteja no modo HA. 2. Verifique se o líder eleito foi identificado. 3. Verifique se o banco de dados LHC está sincronizado. 4. Verifique se `HighAvailabilityServiceControl.psm1` está presente.
Erros de execução remota	1. Verifique se o WinRM está habilitado em todos os Cloud Connectors usando `Test-WSMan -ComputerName <CloudConnectorFQDN>`.

PROBLEMA	SOLUÇÃO
	2. Verifique se as regras do firewall permitem o acesso remoto do PowerShell. 3. Verifique se você tem privilégios de administrador.
A consulta do log de eventos não retorna resultados	1. Verifique se os IDs de Evento estão corretos para o provedor selecionado. 2. Verifique se o intervalo de tempo abrange os eventos esperados.
	Certifique-se de que os limites de tamanho do log de eventos não causaram a sobrescrita de eventos antigos.

Melhores práticas

Siga estas melhores práticas para aproveitar ao máximo a ferramenta e operar seu ambiente de Cache de Host Local com segurança.

Monitoramento regular

- Execute **Descobrir Cloud Connectors** e **Identificar Líder Eleito** periodicamente.
- Monitore os eventos `ConfigSync` (503, 504, 505) para problemas de sincronização.

Análise do log de eventos

- Consulte os últimos 7 dias de eventos de HA para entender os padrões de interrupção.
- Procure pelo ID de Evento 3507 durante o modo HA para estatísticas detalhadas.

Comandos do Broker

- Execute apenas no líder eleito.
- Limite a seleção de propriedades para melhorar o desempenho.
- Use o parâmetro `MaxRecordCount` para ambientes grandes.

Modo de interrupção

- Use o modo de interrupção forçada apenas para testes ou manutenção planejada.
- Sempre verifique se o banco de dados LHC está sincronizado antes de habilitar.
- Desative o modo de interrupção forçada assim que a conectividade primária for restaurada.

Segurança

- Execute com contas de privilégio mínimo sempre que possível.
- Use canais seguros para execução remota.
- Audite as alterações do modo de interrupção.

Exemplos

Os exemplos a seguir assumem que você criou uma pasta em `C:\Reports` para armazenar a saída.

Exemplo 1: Relatório diário do modo HA

```
# Import module

. "C:\Program
Files\Citrix\Broker\Service\LHCVisibilityToolScripts\LHCVisibilityTool.ps1
"



# Discover environment

$connectors = Get-CloudConnectorsInZone

Write-Host "Found $($connectors.Count) Cloud Connectors"



# Check HA status
```

```
$leader = Get-ElectedLeader

if ($leader) {

    Write-Host "System is in HA mode. Elected leader: $leader"



    # Get HA summary events from elected leader

    $events = Get-LHCEventLogs -ComputerName "ElectedLeader" `

        -EventID @(3507, 3508) `

        -ProviderName "Citrix High Availability Service" `

        -StartTime (Get-Date).AddHours(-24) `

        -MaxEvents 100



    # Export to file

    $events[$leader].Events | Select-Object TimeCreated, Id,
LevelDisplayName, Message | Export-Csv -Path "C:\Reports\HA-Status-$(Get-
Date -Format 'yyyyMMdd').csv" -NoTypeInformation

} else {

    Write-Host "System is in normal operations mode"

}
```

Exemplo 2: Verificar o status do ConfigSync em todos os conectores

```
. "C:\Program
Files\Citrix\Broker\Service\LHCVisibilityToolScripts\LHCVisibilityTool.ps1
"
```

```
$results = Get-LHCEventLogs -ComputerName "All" `

    -EventID @(503, 504, 505) `

    -ProviderName "Citrix ConfigSync Service" `

    -StartTime (Get-Date).AddHours(-6) `

    -MaxEvents 10



foreach ($computer in $results.Keys) {

    $lastEvent = $results[$computer].Events | Sort-Object TimeCreated
-Descending | Select-Object -First 1

    $status = switch ($lastEvent.Id) {

        503 { "In Progress" }

        504 { "Success" }

        505 { "Failed" }

    }

    Write-Host "$computer - Last Sync: $($lastEvent.TimeCreated) - Status:
$status"

}
```

Exemplo 3: Obter contagem de sessões durante o modo HA

```
. "C:\Program
Files\Citrix\Broker\Service\LHCVisibilityToolScripts\LHCVisibilityTool.ps1
"



# Ensure we have an elected leader
```

```
$leader = Get-ElectedLeader

if ($leader) {

    # Get all sessions

    $sessions = Invoke-BrokerCommand -Command "Get-BrokerSession"

    Write-Host "Total Sessions: $($sessions.Count)"



    # Group by state

    $sessionsByState = $sessions | Group-Object SessionState

    foreach ($group in $sessionsByState) {

        Write-Host "  $($group.Name): $($group.Count)"

    }

} else {

    Write-Host "Not in HA mode - cannot query sessions from LHC"

}
```

Cenários avançados

Os cenários a seguir combinam várias funções da ferramenta em scripts para operações mais complexas, como automatizar testes de interrupção e exportar dados históricos do modo HA.

Automatizar testes de interrupção

```
# Enable outage mode

Write-Host "Enabling forced outage mode..."

$enableResults = Set-LHCOutageMode -Enable

$allEnabled = $enableResults.Values | Where-Object { -not $_.Success }
```

```
if ($allEnabled) {

    Write-Host "WARNING: Some connectors failed to enable outage mode -
aborting test" -ForegroundColor Yellow

    return

}

Start-Sleep -Seconds 30



# Verify elected leader

$leader = Get-ElectedLeader

Write-Host "Elected leader: $leader"



# Test brokering

$machines = Invoke-BrokerCommand -Command "Get-BrokerMachine" -Properties
@("MachineName", "RegistrationState")

Write-Host "Retrieved $($machines.Count) machines"



# Disable outage mode

Write-Host "Disabling forced outage mode..."

$disableResults = Set-LHCOutageMode
```

Exportar histórico do modo HA

```
$haEvents = Get-LHCEventLogs -ComputerName "All" `

    -EventID @(3502, 3503) `
```

```
    -ProviderName "Citrix High Availability Service" `
    -StartTime (Get-Date).AddDays(-30) `
    -MaxEvents 1000


$report = foreach ($computer in $haEvents.Keys) {
    if (-not $haEvents[$computer].Success) { continue }
    foreach ($event in $haEvents[$computer].Events) {
        [PSCustomObject]@{
            Computer  = $computer
            EventID   = $event.Id
            EventType = if ($event.Id -eq 3502) { "Entered HA Mode" } else
{ "Exited HA Mode" }
            Time      = $event.TimeCreated
        }
    }
}
$report | Sort-Object Time | Export-Csv -Path "C:\Reports\HA-History.csv"
-NoTypeInformation
```

Configurações do servidor de log

Configure as configurações do servidor de log, incluindo o endereço do servidor, a porta e o escopo de log. O **Monitor** usa essas configurações para se conectar ao servidor de log e recuperar logs para monitoramento e solução de problemas.

Para concluir esta tarefa, siga estas etapas:

1. Faça login no **Web Studio** e selecione **Settings** no painel esquerdo.
2. Se nenhum servidor de log estiver configurado, clique em **Add** no bloco **Log server**.
3. Na página **Log server**, insira o **Log server address** e a **Port**.
4. Para definir quais VDAs encaminham logs para o servidor de log, siga estas etapas:
    a. Selecione **Select delivery groups**. Por padrão, **All delivery groups** é selecionado, o que encaminha logs em VDAs em todos os grupos de entrega para o servidor de log.
    b. Para encaminhar logs apenas em VDAs em grupos de entrega específicos, selecione **Select specific delivery groups** e, em seguida, escolha os grupos que deseja incluir.
5. Selecione a **zone** onde o servidor de log reside.
6. Insira a **Authkey** gerada pelo servidor de log. O **Monitor** usa essa chave para autenticar e recuperar logs do servidor.
7. Clique em **Save** para aplicar a configuração. Para atualizar o servidor de log ou modificar o escopo de log, clique em **Edit** no bloco **Settings > Log server**.

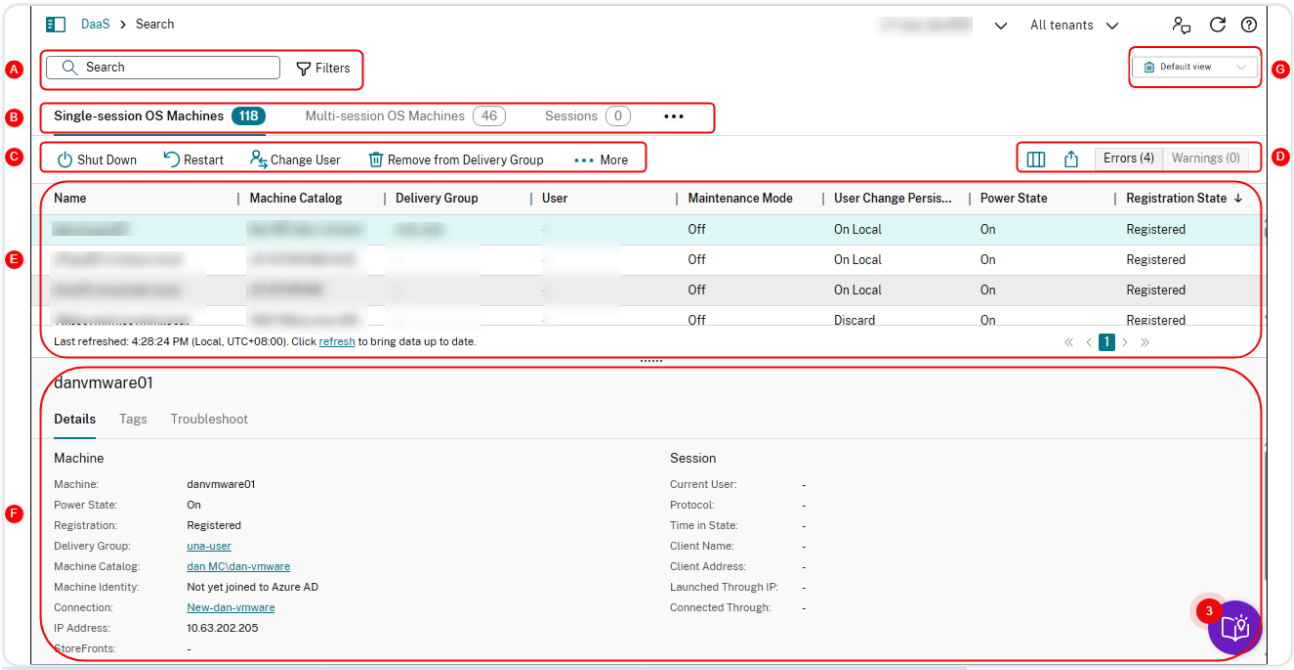
Máquinas e sessões (Pesquisar > Exibição padrão)

Este artigo orienta você sobre como monitorar e gerenciar máquinas e sessões usando a Exibição padrão dentro do nó **Pesquisar**. Ele contém os seguintes tópicos:

- Saiba mais sobre a Exibição padrão
- Pesquisar máquinas e sessões
- Personalizar colunas para exibir
- Gerenciar máquinas e sessões
- Exportar dados de máquina ou sessão para arquivos CSV

Saiba mais sobre a exibição padrão

A exibição padrão dentro do nó **Pesquisar** fornece um local central para monitorar e gerenciar máquinas e sessões de usuário.



CHAMADA	ÁREA	DESCRIÇÃO
A	Barra de pesquisa	Fornece uma pesquisa rápida e uma pesquisa baseada em filtro que permite definir critérios de pesquisa complexos. Para obter mais informações, consulte Pesquisar instâncias.
B	Guias de tipo	Exibe guias para listar máquinas por tipo ou listar todas as sessões. As contagens de instâncias aparecem nos nomes das guias.
C	Ações no nível da instância	Exibe as ações que você pode executar nas *instâncias* selecionadas (máquinas ou

CHAMADA	ÁREA	DESCRIÇÃO
		sessões). Para obter mais informações, consulte Ações da máquina e Ações da sessão.
D	Ações no nível da lista	Exibe as ações que você pode executar na *lista* atual • Ícone de **Exportar**: Exporta a lista de instâncias exibidas na visualização principal para um arquivo CSV. • Ícone **Coluna a ser exibida**: Personalize a exibição principal da lista. • Rótulo **Erros**: Ative este rótulo para exibir apenas máquinas não registradas com erros na exibição principal. Para visualizar os detalhes do

CHAMADA	ÁREA	DESCRIÇÃO
		problema, vá para a guia **Solucionar problemas** no painel **Detalhes**. • Rótulo **Aviso**: Ative este rótulo para exibir apenas máquinas não registradas com avisos na exibição principal. Para visualizar os detalhes do problema, vá para a guia **Solucionar problemas** no painel **Detalhes**.
E	Exibição principal	Exibe as instâncias e suas propriedades. Você pode personalizar a exibição principal selecionando o ícone **Coluna a ser exibida**. Para obter mais informações sobre as colunas disponíveis, consulte Colunas da máquina e Colunas da sessão.

CHAMADA	ÁREA	DESCRIÇÃO
F	Painel de detalhes	Exibe os seguintes detalhes: • Detalhes da instância selecionada (máquina ou sessão) • Tags aplicadas à máquina selecionada • Detalhes de erros ou avisos com a máquina selecionada, incluindo problemas, possíveis causas e soluções sugeridas
G	Alternar para a visualização de Hardware	Clique para alternar da visualização Padrão para a visualização de Hardware.

Pesquisar instâncias

Use a função de pesquisa para localizar máquinas e sessões específicas:

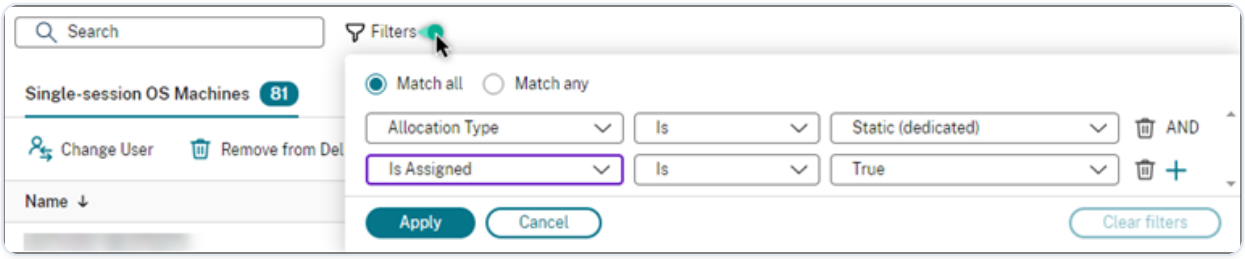
- Pesquisar usando filtros
- Salvar o conjunto de filtros atual para uma pesquisa rápida
- Fixar um campo de filtro na barra de pesquisa
- Pesquisar usando a caixa de pesquisa rápida

- Dicas para aprimorar uma pesquisa

Pesquisar usando filtros

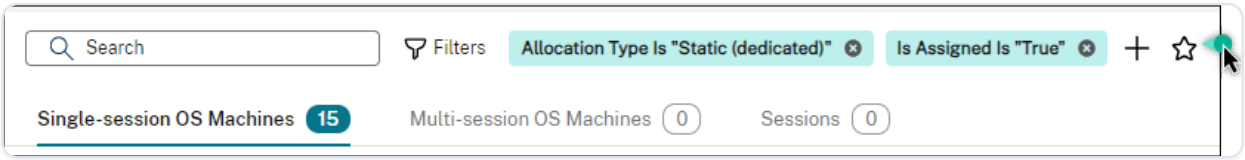
Por exemplo, para localizar todas as máquinas OS de sessão única que são *estáticas* e *atribuídas a usuários*, siga estas etapas:

1. Na guia **Máquinas OS de sessão única**, clique no ícone **Filtros**. O painel Filtros é exibido.
2. Adicione os critérios de filtro necessários.



3. Selecione **Corresponder a todos** (operador AND) se quiser que a pesquisa retorne resultados que correspondam a todos os critérios de filtro. Selecione **Corresponder a qualquer um** (operador OR) se quiser que a pesquisa retorne resultados que correspondam a qualquer um dos critérios de filtro.
4. Clique em **Aplicar**.

   A lista filtrada exibe todas as máquinas OS de sessão única que são estáticas e atribuídas a usuários.

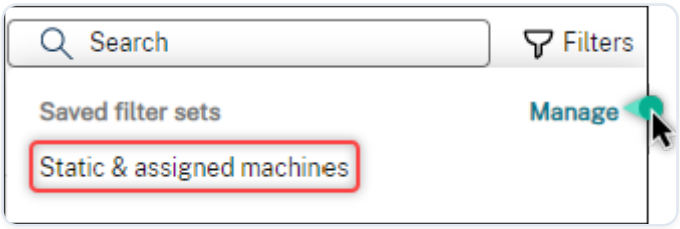


Salvar o conjunto de filtros atual para uma pesquisa rápida

Por exemplo, para salvar o conjunto de filtros para máquinas OS de sessão única que são estáticas e atribuídas a usuários para uso futuro, siga estas etapas:

1. Depois de realizar uma pesquisa baseada em filtro, clique no ícone **Estrela** na barra de pesquisa, conforme mostrado na figura anterior.
2. Na página que aparece, insira um nome para este conjunto de filtros (por exemplo, *Máquinas estáticas e atribuídas*).
3. Clique em **Salvar**.

   O conjunto de filtros salvo aparece na lista de histórico de pesquisa quando você clica na caixa de pesquisa.



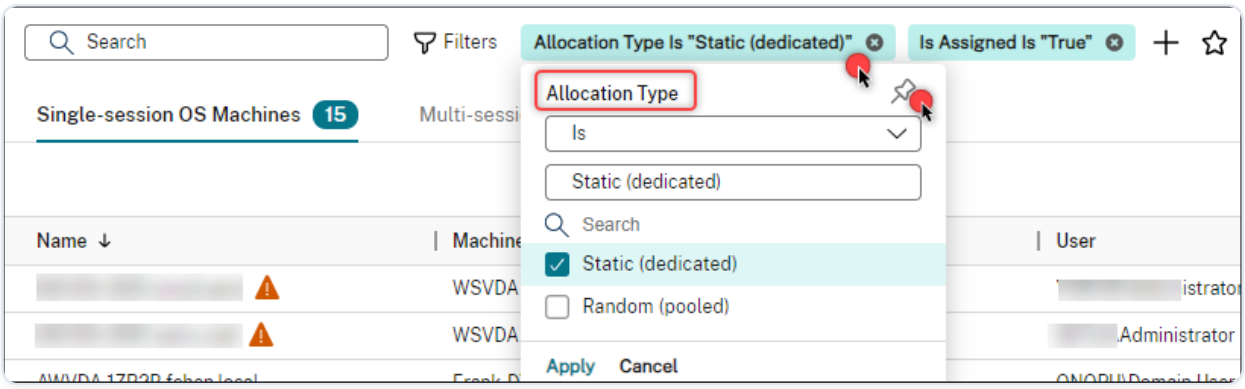
Nota:

Conjuntos de filtros são salvos por conta de usuário. Para gerenciar conjuntos de filtros salvos, selecione **Gerenciar**.

Fixar um campo de filtro na barra de pesquisa

Fixe *campos* de filtro usados com frequência na barra de pesquisa para facilitar o acesso. Por exemplo, após realizar uma pesquisa baseada em filtro, você deseja fixar **Tipo de Alocação** na barra de pesquisa. Siga estas etapas:

1. Clique na *configuração de filtro* na barra de pesquisa.
2. No painel que aparece, clique no ícone **Fixar** para fixar o campo de filtro (*Tipo de Alocação* para este exemplo) na barra de pesquisa.



Pesquisar usando a caixa de pesquisa rápida

A caixa de pesquisa rápida oferece uma maneira conveniente de pesquisar instâncias com base em propriedades relacionadas ao nome ou conjuntos de filtros salvos. As etapas detalhadas são as seguintes:

1. Clique na caixa de pesquisa. Suas pesquisas recentes e conjuntos de filtros salvos aparecem na lista suspensa. Você pode clicar em uma pesquisa anterior ou conjunto de filtros para uma pesquisa rápida.
2. Para iniciar uma nova pesquisa, insira um nome completo ou parcial das seguintes opções:

- Nome da máquina ou nome DNS
- Nome do catálogo de máquinas
- Nome do grupo de entrega
- Nome de usuário da sessão
- Nome do cliente da sessão
- Nome amigável da VM que hospeda a sessão, conforme usado pelo seu hipervisor
- Nome do servidor de hospedagem

Dicas para aprimorar uma pesquisa

Considere as seguintes dicas ao usar o recurso Pesquisar:

- No nó **Pesquisar**, selecione qualquer coluna para classificar os itens.
- Para mostrar mais características a serem incluídas na exibição onde você pode pesquisar e classificar, selecione **Colunas a Exibir** ou clique em qualquer coluna e selecione **Colunas a Exibir**. Na janela **Colunas a Exibir**, marque a caixa de seleção ao lado dos itens que deseja exibir e selecione **Salvar** para sair.

  > **Nota:**
  >
  > As colunas que degradam o desempenho são marcadas com o rótulo **Degrada o desempenho**.

- Para localizar um dispositivo de usuário conectado a uma máquina, use **Cliente (IP)** e **É**, e insira o endereço IP do dispositivo.
- Para localizar sessões ativas, use **Estado da Sessão**, **É** e **Conectado**.
- Para listar todas as máquinas em um grupo de entrega, selecione **Grupos de Entrega** no painel esquerdo. Selecione o grupo e, em seguida, selecione **Exibir Máquinas** na barra de ações ou no menu de contexto.
- Para restringir rapidamente as máquinas provisionadas por MCS por propriedades específicas, use a barra **Pesquisar** disponível em visualização de Hardware.

Tenha as seguintes considerações em mente ao realizar operações de classificação:

- Enquanto o número de itens não exceder 5.000, você pode clicar em qualquer coluna para classificar os itens nela. Quando o número exceder 5.000, você só poderá classificar por nome

ou por usuário atual (dependendo da guia em que você está). Para habilitar a classificação, use filtros para reduzir o número de itens para 5.000 ou menos.

- Quando o número de itens é maior que 500, mas não mais que 5.000:
  - Armazenamos todos os dados em cache localmente para melhorar o desempenho da classificação. Nas guias **Máquinas OS de sessão única** e **Máquinas OS de várias sessões**, armazenamos os dados em cache na primeira vez que você clica em uma coluna (qualquer coluna, exceto a coluna **Nome**) para classificar. Na guia **Sessões**, armazenamos os dados em cache na primeira vez que você clica em uma coluna (qualquer coluna, exceto a coluna **Usuário Atual**) para classificar. Como resultado, a classificação leva mais tempo para ser concluída. Para um desempenho mais rápido, classifique por nome ou usuário atual, ou use filtros para reduzir o número de itens.
  - A seguinte mensagem abaixo da tabela indica que os dados estão em cache: Última atualização: `<the time when you refreshed the table>`. Nesse caso, as operações de classificação são baseadas em itens que foram carregados anteriormente. Esses itens podem não estar atualizados. Para atualizá-los, clique no ícone de atualização.

Personalizar colunas a serem exibidas

Crie uma exibição principal personalizada para exibir as propriedades e status cruciais para suas operações diárias. As etapas detalhadas são as seguintes:

1. No nó **Pesquisar**, selecione a guia **Máquinas OS de várias sessões**, **Máquinas OS de sessão única** ou **Sessões**, conforme necessário.
2. Clique no ícone **Colunas a serem exibidas** na barra de ações e selecione as colunas.

   Para obter mais informações sobre as colunas disponíveis e suas descrições, consulte Colunas da máquina e Colunas da sessão.

Ao escolher as colunas, você pode ver colunas marcadas com o rótulo **Degrada o desempenho**. A seleção dessas colunas pode degradar o desempenho do console. Tenha estas considerações em mente:

- Depois de concluir sua personalização, a tabela é atualizada para exibir as colunas selecionadas. A presença delas pode resultar em atrasos ao atualizar a tabela.
- Depois de atualizar o navegador ou sair do console e fazer login novamente, uma mensagem aparece perguntando se deseja preservar essas colunas. Se você optar por preservá-las, estará restrito a atualizar a tabela mais de uma vez por minuto para um desempenho ideal do

console. Para atualizações mais frequentes, remova todas as colunas que degradam o desempenho.

Gerenciar máquinas e sessões

Use as ações no nó Pesquisar para solucionar problemas de máquinas e sessões ou processar solicitações de usuários.

É bom saber

Você pode gerenciar máquinas em diferentes níveis:

- No nível da máquina individual. Use o nó **Pesquisar** para localizar máquinas de destino e executar ações.
- No nível do catálogo de máquinas, como alterar imagens mestre para um catálogo, excluir máquinas de um catálogo e adicionar máquinas a um catálogo. Para obter mais informações, consulte Gerenciar catálogos de máquinas.
- No nível do grupo de entrega, como ativar ou desativar o modo de manutenção para máquinas em um grupo. Para obter mais informações, consulte Gerenciar grupos de entrega.

Além do nível de sessão individual, você também pode gerenciar sessões no nível do grupo de entrega, como configurar o pré-lançamento e a permanência da sessão para um grupo de entrega. Para obter mais informações, consulte Gerenciar Grupos de Entrega.

Executar ações em máquinas ou sessões

Para gerenciar máquinas ou sessões no nível da instância individual, siga estas etapas:

1. No nó **Pesquisar**, selecione a guia **Máquinas OS multissessão**, **Máquinas OS de sessão única** ou **Sessões**.
2. Selecione uma ou mais instâncias conforme necessário.
3. Na barra de ações ou no menu de clique com o botão direito, selecione uma ação com base nos problemas que você encontrar com essas instâncias ou nas solicitações do usuário.

   Para obter mais informações sobre as ações disponíveis e suas descrições, consulte Ações da máquina e Ações da sessão.

> **Nota:**

> Se você selecionar duas ou mais instâncias, somente as ações que se aplicam a todas elas estarão disponíveis.

Exportar dados de máquina ou sessão para arquivos CSV

Exporte a lista de instâncias (máquinas ou sessões) exibidas em uma guia (até 30.000 itens) para um arquivo CSV. As etapas detalhadas são as seguintes:

1. No nó **Pesquisar**, selecione a guia **Máquinas OS multissessão**, **Máquinas OS de sessão única** ou **Sessões** conforme necessário.
2. Clique no ícone **Exportar** no canto superior direito.
3. Na caixa de diálogo que aparece, clique em **Continuar**.

   A exportação pode levar vários minutos para ser concluída. Você pode encontrar o arquivo na pasta de download padrão do seu navegador.

> **Nota:**
>
> Em cada guia do nó **Pesquisar**, você não pode realizar outra exportação enquanto uma exportação estiver em andamento.

Ações e colunas da máquina

Este artigo lista as ações da máquina, as colunas da máquina e suas descrições.

Ações

Visualize as ações que você pode realizar nas máquinas e suas descrições. Algumas ações suportam a operação **Selecionar tudo**, permitindo que você aplique a ação a todas as máquinas em todas as páginas.

AÇÃO	DESCRIÇÃO	APLICA-SE A
Executar Verificação de Integridade	Disponível apenas para VDAs Windows registrados, versão 2019 ou posterior. Execute uma verificação de integridade em uma	Sessão única e multi-sessão

AÇÃO	DESCRIÇÃO	APLICA-SE A
	máquina. Para obter mais informações sobre o conteúdo da verificação, consulte Sobre as verificações de integridade.	
Remover do Grupo de Entrega	Remove uma máquina do grupo de entrega.	Sessão única e multi-sessão
Adicionar ao Grupo de Entrega	Adiciona uma máquina a um grupo de entrega.	Sessão única e multissessão
Exibir Sessões	Exibir as sessões em execução em uma máquina	Sessão única e multissessão
Gerenciar Tags	Adicione e gerencie tags para uma máquina. Para obter mais informações sobre casos de uso típicos de tags, consulte Tags.	Sessão única e multissessão
Ativar Modo de Manutenção	Coloque uma máquina em modo de manutenção antes de aplicar patches ou para solução de problemas.	Sessão única e multissessão
	Este modo impede que novas conexões sejam feitas a essa máquina. Os usuários podem se conectar a sessões	

AÇÃO	DESCRIÇÃO	APLICA-SE A
	existentes nessa máquina, mas não podem iniciar novas sessões nela.	
Desativar Modo de Manutenção	Desative o modo de manutenção para uma máquina.	Sessão única e multissessão
Atualizar VDA	Atualizar VDA para uma máquina.	Máquinas de SO de sessão única ou multissessão que atendem a determinados requisitos: Saiba mais.
Fazer logoff	Forçar logoff de uma máquina	Sessão única e multissessão
Excluir	Excluir uma VM de um catálogo de máquinas, deixando-a intacta no hipervisor ou serviço de nuvem.	Sessão única e multissessão
Alterar Usuário	Atribuir uma máquina a um usuário específico.	máquinas *estáticas* de sessão única.
Iniciar	Iniciar uma máquina.	Sessão única e multissessão
Desligar	Desligar uma máquina.	Sessão única e multissessão
Reiniciar	Reiniciar uma máquina	Sessão única e multissessão
Suspender	Colocar uma máquina em estado	Máquinas de SO de sessão única

AÇÃO	DESCRIÇÃO	APLICA-SE A
	de hibernação ou suspensão. Ao suspender uma máquina, o DaaS armazena o conteúdo da memória da máquina em um arquivo e, em seguida, desliga a máquina.	
Retomar	Retomar uma máquina suspensa. Ao retomar uma máquina suspensa, o DaaS inicia a máquina e a restaura para o estado anterior.	Máquinas de SO de sessão única
Forçar Reinicialização	Forçar a reinicialização de uma máquina.	Máquinas OS de sessão única
Forçar Desligamento	Forçar o desligamento de uma máquina.	Máquinas OS de sessão única
Visualizar no Monitor	Abrir a visualização detalhada de uma máquina no Monitor. Esta ação está disponível apenas para funções com a permissão de página **Director > Gerenciar > Visualizar Detalhes da Máquina**.	Máquinas OS de sessão única e multissessão

Colunas

Visualize todas as colunas da máquina e suas descrições por tipo:

- Máquina
- Detalhes da máquina
- Aplicativos
- Hospedagem
- Conexão
- Registro
- Detalhes da Sessão
- Sessão

Máquina

Colunas na categoria **Máquina**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Nome	O nome de host DNS da máquina.	Sessão única e multi-sessão
Catálogo de Máquinas	O nome do catálogo ao qual a máquina pertence.	Sessão única e multissessão
Grupo de Entrega	O nome do grupo de entrega ao qual a máquina pertence.	Sessão única e multissessão
Nome de Exibição do Usuário	Os nomes completos dos usuários associados à máquina (geralmente no formato `Firstname Lastname`). Usuários associados são os usuários atuais para máquinas	Sessão única e multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	compartilhadas e os usuários atribuídos para máquinas dedicadas.	
Usuário	Os nomes de usuário dos usuários associados à máquina (no formato “domínio\usuário”). Usuários associados são os usuários atuais para máquinas compartilhadas e os usuários atribuídos para máquinas dedicadas.	Sessão única e multissessão
Nome Principal do Usuário	Os Nomes Principais de Usuário dos usuários associados à máquina (no formato “usuário@domínio”). Usuários associados são os usuários atuais para máquinas compartilhadas e os usuários atribuídos para máquinas dedicadas.	Sessão única e multissessão
Nome de Exibição da Área de Trabalho	O nome publicado da máquina originalmente usada para iniciar a sessão. É o nome exibido no aplicativo Citrix	Somente sessão única

COLUNA	DESCRIÇÃO	APLICA-SE A
	Workspace™ ou no StoreFront.	
	Nota: Para alterar a exibição de um desktop, você precisa da permissão **Perform Machine Update** porque a alteração do nome de exibição envolve a atualização da propriedade da máquina.	
Condições do Desktop	A lista de condições pendentes do desktop para a máquina. Valores possíveis: Unknown, CPU, ICALatency e UPMLogonTime.	Sessão única e multi-sessão
Tipo de Alocação	O tipo de alocação da máquina: **Permanente**, quando alocada a um usuário permanentemente. **Aleatória**, quando alocada aleatoriamente.	Sessão única e multi-sessão
Modo de Manutenção	Indica se a máquina está no modo de manutenção.	Sessão única e multi-sessão
Configuração de Conexão do Windows	Modo de logon relatado pelo Windows.	Somente multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	Valores possíveis: LogonEnabled, Draining, DrainingUntilRestart e LogonDisabled.	
Está Atribuído	Indica se um desktop dedicado foi atribuído a um usuário ou a um cliente (nome/endereço). Os usuários podem ser atribuídos explicitamente ou por atribuição no primeiro uso da máquina.	Sessão única e multissessão
É Físico	Indica se a máquina é física ou não. `True` indica que a máquina é física, o que significa que não é gerenciada por energia pelo DaaS. `False` indica o contrário.	Sessão única e multissessão
Tipo de Provisionamento	Como a máquina foi provisionada. Valores possíveis: • Manual: Não provisionado usando PVS ou MCS.	Sessão única e multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	PVS: Provisionado usando PVS (máquinas físicas, blade e virtuais)	
	MCS: Provisionado usando MCS (somente VMs)	
Reinicialização Agendada ^	O estado de qualquer operação de reinicialização agendada para a máquina. Valores possíveis	Sessão única e multissessão
	Nenhum: Nenhuma reinicialização está agendada.	
	Pendente: Aguardando reinicialização, mas está disponível para uso. • Drenando: Aguardando reinicialização e está indisponível para novas sessões. No entanto, reconexões a conexões existentes ainda são permitidas.	

COLUNA	DESCRIÇÃO	APLICA-SE A
	• Em Andamento: Em andamento ativo de uma reinicialização agendada. • Natural: Reinicialização natural em andamento. A máquina está aguardando uma reinicialização.	
Zona	O nome da zona onde a máquina está localizada.	Sessão única e multi-sessão
Estado	O estado geral da área de trabalho associada à máquina, derivado de vários estados específicos, como estado da sessão, estado de registro e estado de energia.	Sessão única e multi-sessão
	Estados possíveis: Desligado, Não Registrado, Disponível, Desconectado, EmUso e Preparando.	

COLUNA	DESCRIÇÃO	APLICA-SE A
Tags	A lista de tags associadas à máquina.	Sessão única e multi-sessão
Atualização do VDA	O estado da máquina para ações de atualização de pacote VDA.	Sessão única e multi-sessão
	Valores possíveis: Agendado, Não configurado, Disponível, Atualizado, Desconhecido.	
Status da Atualização do VDA	O status para ações de atualização do VDA. Valores possíveis: Agendado, Aguardando atualização, Em andamento, Cancelado, Falha na atualização, Bem-sucedido, Falha na validação, Desconhecido	Sessão única e multissessão
Capaz de Suspender	Indica se a máquina suporta ações de energia (Suspender e Retomar).	Sessão única e multissessão
Índice do Avaliador de Carga	O índice de carga atual. O índice de carga efetivo geral (porcentagem) para a máquina. Para	Somente multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	obter mais informações, consulte CTX202150.	
Índice de Carga	O índice de carga atual. Para obter mais informações, consulte Saiba mais.	Somente multissessão
Estado de Esvaziamento	Indica se a máquina está esvaziando e será desligada após o término de todas as sessões na máquina. 'True' aparece apenas para máquinas multissessão gerenciadas por energia.	Somente multissessão
	Nota: A máquina não desliga se estiver em modo de manutenção. Ela desliga somente depois de sair do modo de manutenção.	
Cloud Connector	O nome do Cloud Connector através do qual a máquina é proxy.	Sessão única e multissessão

Detalhes da máquina

Colunas na categoria **Detalhes da máquina**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Versão do Agente	A versão do Citrix Virtual Delivery Agent (VDA) instalado na máquina.	Sessão única e multissessão
Endereço IP	O endereço IP da máquina.	Sessão única e multi-sessão
Atribuído	Indica se um desktop dedicado foi atribuído a um usuário ou a um cliente (nome/endereço). Os usuários podem ser atribuídos explicitamente ou por atribuição no primeiro uso da máquina.	Sessão única e multi-sessão
Tipo de SO	O tipo de sistema operacional em execução na máquina.	Somente sessão única

Aplicativos

Colunas na categoria **Aplicativos**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Aplicativo em Uso	A lista de aplicativos em uso na máquina (exibidos como nomes de navegador).	Sessão única e multissessão
Aplicativos Publicados	A lista de aplicativos publicados pela máquina (exibidos como nomes de navegador).	Sessão única e multissessão

Conexões

Colunas na categoria **Conexões**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Cliente (IP)	O endereço IP do cliente conectado à máquina.	Somente sessão única

COLUNA	DESCRIÇÃO	APLICA-SE A
Cliente	O nome do host do cliente conectado à máquina.	Somente sessão única
Versão do Plug-In	A versão do aplicativo Citrix Workspace no cliente conectado.	Somente sessão única
Conectado Via	O nome do host da conexão de entrada, geralmente um gateway, roteador ou cliente.	Somente sessão única
Conectado Via (IP)	O endereço IP da conexão de entrada, geralmente um gateway, roteador ou cliente.	Somente sessão única
Tipo de Conexão	O protocolo usado para a sessão. Valores possíveis: HDX, RDP e Console. Nota: O campo é deixado em branco para sessões de console em VDAs do XenDesktop® 5.	Somente sessão única
Hora da Última Conexão (UTC)	A hora da última tentativa de conexão detectada que falhou ou foi bem-sucedida.	Sessão única e multissessão
Último Usuário de Conexão	O nome SAM (no formato “DOMÍNIO\usuário”) do usuário que tentou uma conexão com a máquina pela última vez. Se o nome SAM não estiver disponível, o SID será usado.	Sessão única e multissessão
Secure ICA® Ativo	Indica se o SecureICA está ativo na sessão atual. Sempre nulo para máquinas multissessão.	Sessão única e multissessão

Hospedagem

Colunas na categoria **Hospedagem**.

COLUNA	DESCRIÇÃO	APLICA-SE A
VM	O nome amigável de uma máquina hospedada executando a sessão, conforme usado por seu hipervisor. Não corresponde necessariamente ao nome DNS ou AD da máquina.	Sessão única e multissessão
Nome do Servidor de Hospedagem	O nome DNS do hipervisor que está hospedando a máquina, se gerenciado.	Sessão única e multi-sessão
Conexão	O nome da conexão do host atribuída à máquina que hospeda a sessão.	Sessão única e multi-sessão
Atualização Pendente	Indica se a imagem da VM para uma máquina hospedada está desatualizada e deve ser atualizada para uma nova imagem na próxima reinicialização da máquina.	Sessão única e multi-sessão
Persistência de Alterações do Usuário	Como as alterações do usuário são tratadas, indicando	Sessão única e multi-sessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	se as alterações são persistentes: • OnLocal: Persistente. As alterações do usuário são salvas localmente. • Descartar: Não persistente. As alterações do usuário são descartadas.	
Ação de Energia Pendente	Indica se há alguma ação de energia pendente para a máquina.	Sessão única e multi-sessão
Estado de Energia	O estado de energia da máquina. Valores possíveis: Não gerenciado, Desconhecido, Indisponível, Desligado, Ligado, Suspenso, Ligando, Desligando, Suspendendo e Retomando.	Sessão única e multi-sessão
Será Desligado Após o Uso	Aplicável apenas a máquinas de sessão única gerenciadas por energia. Indica se a máquina está comprometida e será desligada após o	Somente sessão única

COLUNA	DESCRIÇÃO	APLICA-SE A
	término de todas as sessões.	
	Observação: A máquina não será desligada se estiver em modo de manutenção. Ela será desligada somente depois que for retirada do modo de manutenção.	

Registro

Colunas na categoria **Registro**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Última Falha de Registro	O motivo da última desativação do registro da máquina com o broker.	Sessão única e multi-sessão
	Os valores possíveis são: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrat	

COLUNA	DESCRIÇÃO	APLICA-SE A
	ionCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError e BrokerRegistrationLimitReached.	
Hora da Última Falha de Registro (UTC)	A hora da última desativação do registro da máquina.	Sessão única e multi-sessão
Estado do Registro	O estado de registro da máquina. Valores possíveis: Não registrado, Inicializando, Registrado e Erro do Agente.	Sessão única e multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
Estado de Falha	O estado de resumo de qualquer estado de falha atual da máquina. Valores possíveis: • Nenhum: Nenhuma falha. A máquina está íntegra. • FalhaAoIniciar: A última operação de inicialização da máquina falhou. • TravadoNaInicialização: A máquina não conseguiu iniciar após ser ligada. • Não registrado. A máquina falhou ao registrar dentro do período esperado ou seu registro foi rejeitado. • Capacidade Máxima. A máquina está se reportando com	Sessão única e multissessão

COLUNA	DESCRIÇÃO	APLICA-SE A
	capacidade máxima.	

Detalhes da sessão

Colunas na categoria **Detalhes da sessão**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Iniciado por	O nome do host do servidor StoreFront usado para iniciar a sessão intermediada atual. Sempre nulo para máquinas multi-sessão.	Sessão única e multi-sessão
Iniciado por (IP)	O endereço IP do servidor StoreFront usado para iniciar a sessão intermediada atual. Sempre nulo para máquinas multi-sessão.	Sessão única e multissessão
Hora da Alteração da Sessão (UTC)	A hora da última alteração de estado da sessão atual.	Somente sessão única
Filtros SmartAccess	Tags Smart Access para a sessão atual. Sempre nulo para máquinas multissessão.	Sessão única e multissessão

Sessão

Colunas na categoria **Sessão**.

COLUNA	DESCRIÇÃO	APLICA-SE A
Estado da Sessão	O estado da sessão atual. Valores possíveis: Other, PreparingSession, Connected, Active, Disconnected, Reconnecting,	Somente sessão única

COLUNA	DESCRIÇÃO	APLICA-SE A
	NonBrokeredSession e Unknown.	
Usuário Atual	O nome do usuário da sessão atual (no formato “DOMÍNIO\usuário”).	Somente sessão única
Hora de Início (UTC)	A hora de início da sessão atual.	Somente sessão única
Contagem de Sessões	O número de sessões na máquina.	Somente multissessão

Ações e colunas de sessão

Este artigo lista as ações de sessão, as colunas de sessão e suas descrições.

Ações

Visualize as ações que você pode executar nas sessões e suas descrições. Algumas ações suportam a operação **Selecionar tudo**, permitindo que você aplique a ação a todas as sessões em todas as páginas.

AÇÃO	DESCRIÇÃO	APLICA-SE A SESSÕES EM
Fazer logoff	Fazer logoff de um usuário de uma sessão.	Máquinas de SO de sessão única ou máquinas de SO de várias sessões
Enviar mensagem	Enviar uma mensagem para o usuário de uma sessão.	Máquinas de SO de sessão única ou máquinas de SO de várias sessões
Visualizar máquinas	Visualizar a máquina host de uma sessão.	Máquinas OS de sessão única ou máquinas OS de múltiplas sessões

AÇÃO	DESCRIÇÃO	APLICA-SE A SESSÕES EM
Desconectar	Desconectar uma sessão. Se uma sessão for desconectada, ela ainda estará ativa e seus aplicativos continuarão a ser executados, mas o dispositivo do usuário não estará mais se comunicando com o DaaS.	Máquinas OS de sessão única ou máquinas OS de múltiplas sessões
Desligar Máquina	Desligar a máquina associada a uma sessão.	Máquinas OS de sessão única
Reiniciar Máquina	Reiniciar a máquina associada a uma sessão.	Máquinas OS de sessão única
Visualizar no Monitor	Abrir a visualização detalhada de uma máquina no Monitor. Esta ação está disponível apenas para funções com a permissão **Director > Manage > View Activity Manager page** ou **Director > Manage > View User Details page**.	Máquinas OS de sessão única e de múltiplas sessões

Colunas

Visualize as colunas da sessão e suas descrições.

COLUNA	DESCRIÇÃO
Usuário atual	O nome do usuário; o Nome Principal de Usuário (UPN) do usuário.
Nome	O nome do host DNS da máquina que hospeda a sessão.
Grupo de Entrega	O nome do grupo de entrega que contém a máquina que hospeda a sessão.
Catálogo de Máquinas	O nome do catálogo de máquinas que contém a máquina que hospeda a sessão.
Versão do Agente	A versão do Citrix Virtual Delivery Agent (VDA) instalado na máquina que hospeda a sessão.
Aplicativo em Uso	A lista de aplicativos em uso na sessão, identificados por seus nomes administrativos.
Intermediação Autônoma	Se esta é uma sessão HDX™ estabelecida por uma conexão direta sem intermediação.
Hora da Intermediação (UTC)	A hora em que a sessão foi intermediada.
Nome de Usuário da Intermediação	O nome do usuário que realizou a intermediação.
Cliente (IP)	O endereço IP do cliente conectado à sessão.

COLUNA	DESCRIÇÃO
Cliente	O nome do host do cliente conectado à sessão.
Versão do Plug-in	A versão do aplicativo Citrix Workspace™ em execução no cliente conectado à sessão.
Conectado Via	O nome do host das conexões de entrada, tipicamente um gateway, roteador ou cliente.
Conectado Via (IP)	O endereço IP da conexão de entrada, tipicamente um gateway, roteador ou cliente.
Tipo de Alocação	Se a sessão é compartilhada ou dedicada.
Oculto	Se a sessão está oculta para o usuário e não deve ser reconectada.
VM	O nome amigável da VM que hospeda a sessão, conforme usado pelo seu hipervisor. Não corresponde necessariamente ao nome DNS ou AD da máquina.
Nome do Servidor de Hospedagem	O nome DNS do hipervisor que está hospedando a máquina de hospedagem da sessão.
Conexão	O nome da conexão de host atribuída à máquina que hospeda a sessão.

COLUNA	DESCRIÇÃO
Atualização Pendente	Se a imagem da VM para uma máquina hospedada está desatualizada e deve ser atualizada para uma nova imagem na próxima reinicialização da máquina.
Modo de Manutenção	Se a máquina que hospeda a sessão está em modo de manutenção.
Endereço IP	O endereço IP da máquina que hospeda a sessão.
É Física	Se a máquina que hospeda a sessão é física ou não. `True` indica que a máquina é física, o que significa que não é gerenciada por energia pelo DaaS. `False` indica o contrário.
Iniciado Via	O nome do host do servidor StoreFront™ usado para iniciar a sessão. Em branco se a sessão foi iniciada via Workspace.
Iniciado Via (IP)	O endereço IP do servidor StoreFront usado para iniciar a sessão. Em branco se a sessão foi iniciada via Workspace.
Tipo de SO	A string de identificação do sistema operacional que hospeda a sessão.
Persistência de Alterações do Usuário	Como as alterações do usuário são tratadas,

COLUNA	DESCRIÇÃO
	indicando se as alterações são persistentes • OnLocal: Persistente. As alterações do usuário são salvas localmente. • Discard: Não persistente. As alterações do usuário são descartadas.
Tipo de Conexão	O protocolo usado para a sessão, como HDX, RDP ou Console. **Nota:** O campo fica em branco para sessões de console em VDAs do XenDesktop® 5.
Tipo de Provisionamento	Como a máquina que hospeda a sessão foi provisionada: • Manual: Não provisionado usando PVS ou MCS. • PVS: Provisionado por PVS (Máquinas físicas, blade e virtuais). • MCS: Provisionado por MCS (Somente VMs).
Secure ICA® Ativo	Se o SecureICA está ativo na sessão.
Estado da Sessão	O estado da sessão. Valores possíveis: Connected, Active ou Disconnected. Outros

COLUNA	DESCRIÇÃO
	estados podem ocorrer para sessões em máquinas com níveis funcionais anteriores a L7, como PreparingSession, Reconnecting, NonBrokeredSession, Other e Unknown.
Hora da Alteração da Sessão	A hora da alteração de estado mais recente para a sessão.
Estado do Aplicativo	O estado dos aplicativos na sessão. Valores possíveis: PreLogon, PreLaunched, Active, Desktop, Lingering e NoApps.
Suporte à Sessão	Se a máquina que hospeda a sessão suporta sessões múltiplas ou únicas.
Zona	Nome da zona onde a máquina que hospeda a sessão está localizada.
Filtros SmartAccess	Tags Smart Access para a sessão.
Hora de Início (UTC)	Quando a sessão foi iniciada.
Estado	O estado de resumo da máquina. Valores possíveis: Não registrado, Desconectado ou Em Uso.
Tempo no Estado (UTC)	Há quanto tempo a sessão está em seu estado atual.
Delivery Controller™	O nome de host DNS do controlador com o qual a

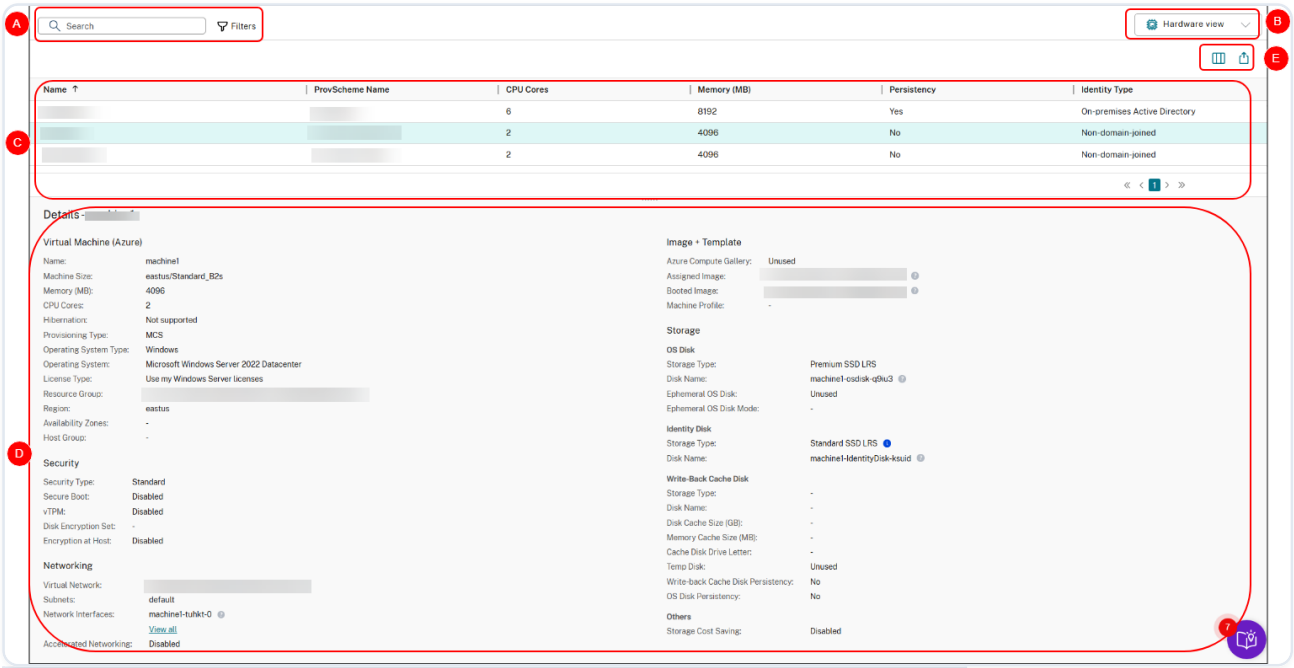
COLUNA	DESCRIÇÃO
	máquina de hospedagem da sessão está registrada.
Nome de Exibição do Usuário	O nome completo do usuário.
Nome de Exibição da Área de Trabalho	O nome publicado da máquina originalmente usada para iniciar a sessão. É o nome exibido no aplicativo Citrix Workspace ou no StoreFront. Para sessões de aplicativo, é o nome do primeiro aplicativo iniciado na sessão, mesmo que esse aplicativo já tenha sido encerrado. O nome permanece inalterado mesmo que o recurso seja posteriormente renomeado ou removido.

Monitorar máquinas provisionadas por MCS em Pesquisar > Visualização de Hardware

Este artigo orienta você sobre como visualizar máquinas provisionadas por MCS e suas propriedades usando a **Visualização de Hardware** dentro do nó **Pesquisar**.

Saiba mais sobre a visualização de hardware

A visualização de hardware dentro do nó **Pesquisar** exibe suas máquinas provisionadas por MCS e suas propriedades críticas, incluindo configurações de segurança da máquina, detalhes de rede, imagens e detalhes do perfil da máquina.



CHAMADA	ÁREA	DESCRIÇÃO
A	Barra de pesquisa	Fornece uma pesquisa rápida e uma pesquisa baseada em filtro que permite definir critérios de pesquisa complexos. Para obter mais informações, consulte Pesquisar máquinas. **Dica:** Use filtros para restringir rapidamente as máquinas por propriedades específicas. Por exemplo, combine **Atualização de Imagem Pendente = Sim** e **Tipo de Identidade = ActiveDirectory** para visualizar

CHAMADA	ÁREA	DESCRIÇÃO
		todas as máquinas do Active Directory que estão aguardando atualizações de imagem.
B	Alternar para a exibição Padrão	Alternar da exibição Hardware para exibição Padrão.
C	Exibição principal	Exibe suas máquinas provisionadas por MCS e suas propriedades críticas. Você pode personalizar a exibição selecionando o ícone **Coluna a ser exibida**. Para obter mais informações sobre as colunas disponíveis, consulte Colunas da máquina.
D	Painel de detalhes	Exibe informações detalhadas para a máquina selecionada.
E	Ações no nível da lista	Exibe as ações que você pode realizar em toda a lista exibida: • Ícone **Exportar**: Exporta a lista

CHAMADA	ÁREA	DESCRIÇÃO
		de máquinas exibidas na exibição principal para um arquivo CSV. • ícone **Coluna a ser exibida**: Personalize a exibição principal da lista.

Referência: Colunas da máquina

Esta tabela lista todas as colunas na exibição Hardware e suas descrições.

COLUNA	DESCRIÇÃO
Nome	O nome do host DNS da máquina.
Nome do Esquema de Provisionamento	O nome do esquema de provisionamento usado para provisionar a máquina.
Núcleos de CPU	O número de núcleos de CPU alocados para a máquina.
Memória (MB)	A quantidade de memória (em MB) alocada para a máquina.
Persistência	Indica se o disco e os dados da máquina persistem entre reinicializações.
Tipo de Identidade	O tipo de identidade da máquina.
Atualização de Imagem Pendente	Indica se a imagem da VM para a máquina está desatualizada e deve ser atualizada para

COLUNA	DESCRIÇÃO
	uma nova imagem na próxima reinicialização da máquina.
Hora da Última Inicialização (UTC)	A data e hora (em UTC) da última inicialização da máquina.
Usar WBC	Indica se a máquina está configurada com WBC (também conhecido como MCSIO).
Tamanho do Disco WBC (GB)	O tamanho do cache de disco MCSIO da máquina.
Tamanho da Memória WBC (MB)	O tamanho do cache de memória MCSIO da máquina.
Provedor de Identidade	O provedor de identidade da máquina.
Tipo de Ativação	Válido apenas para VDAs Windows. O tipo de ativação da licença Windows da máquina. Os valores incluem: VDA não suportado, Serviço de Gerenciamento de Chaves, Chave de Ativação Múltipla e Não válido.

Gerenciamento de vários sites e agregação de recursos de usuário

Como administrador com acesso total a vários sites, você pode designar um site como principal e vincular outros sites a ele para gerenciamento centralizado. Esse recurso ajuda a melhorar a eficiência operacional em vários aspectos:

- **Gerenciamento eficiente de sites**. Os administradores podem gerenciar vários sites a partir de uma única interface, alternando entre eles usando o menu suspenso no canto superior direito.
- **Navegação contínua**. Os administradores podem alternar facilmente entre o Studio e o Monitor sem precisar selecionar novamente o site. Quando um site é selecionado no Studio, ele é automaticamente selecionado no Monitor, otimizando seu fluxo de trabalho.
- **Operações de help desk simplificadas**. Os administradores podem visualizar informações de todos os sites em um único console do Monitor.

- **Recursos agregados para usuários finais**. Os usuários finais podem fazer login em uma única loja (*por exemplo*, primarysite.cloud.com) para acessar seus aplicativos e desktops de qualquer site vinculado.

Este artigo ajuda você a entender, configurar e usar o gerenciamento centralizado de sites. Ele o orienta pelos seguintes tópicos:

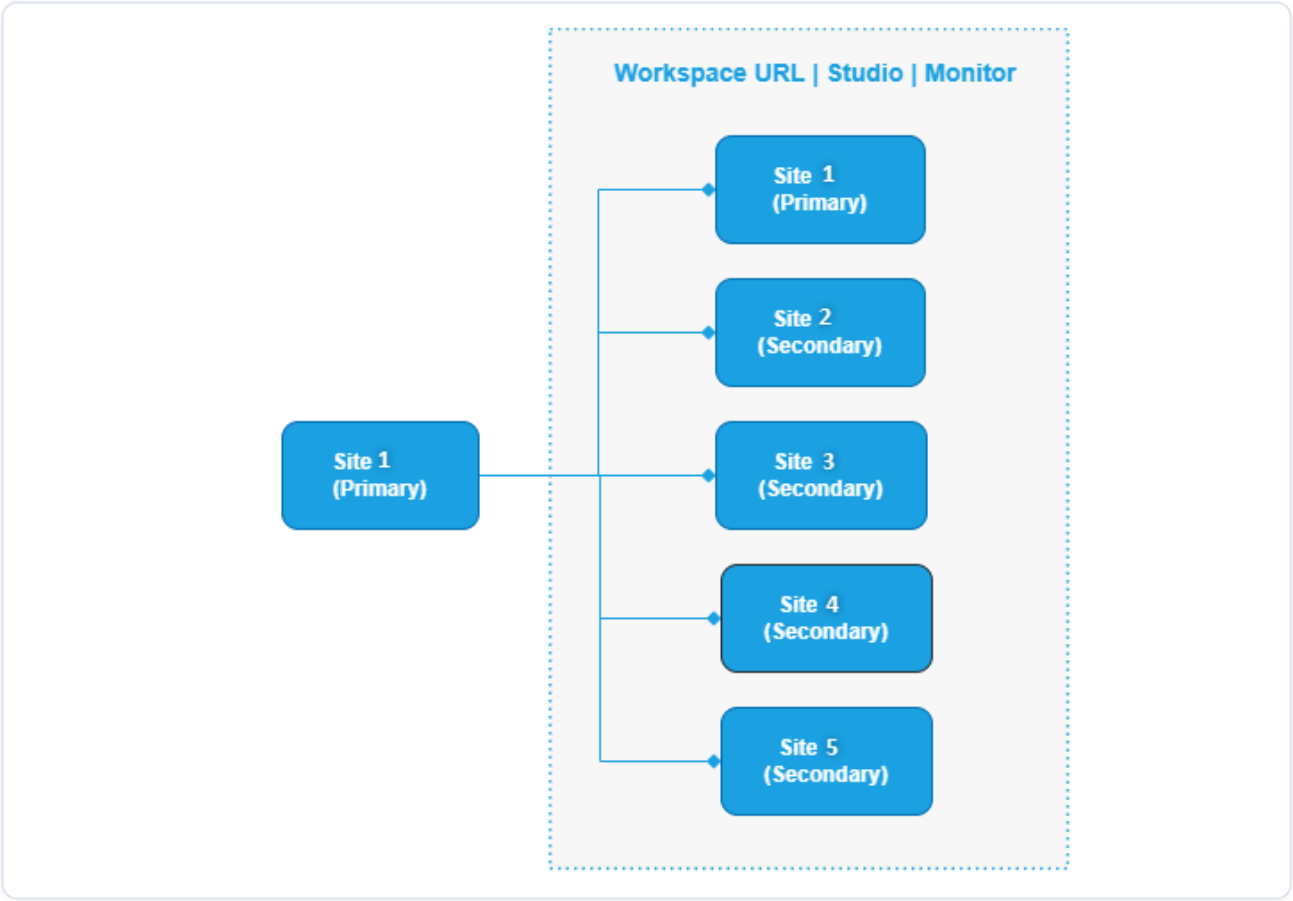
- Visão geral
- Práticas recomendadas para gerenciamento de vários sites
- Administradores com acesso total: Configurar o gerenciamento centralizado de sites
- Administradores: Gerenciar sites a partir de uma única interface
- Casos de uso típicos

> **Nota:**

> O gerenciamento centralizado de sites não é atualmente suportado para Provedores de Serviços Citrix (CSPs) e seus locatários.

Visão geral

O diagrama a seguir ilustra a arquitetura hierárquica primária-secundária no gerenciamento centralizado de sites.



Definições de sites primários e secundários:

- **Primário** (também conhecido como **hub**). O site central usado para gerenciar todos os sites vinculados.
- **Secundário** (também conhecido como **spoke**). Um site adicionado ao site primário para gerenciamento centralizado.

Funções e permissões do administrador

O acesso ao recurso de gerenciamento de vários sites varia de acordo com a função do administrador:

- Apenas administradores com **acesso total** podem configurar o gerenciamento de vários sites e a agregação de recursos do usuário final.
    - Para que os sites sejam gerenciados como sites secundários, o administrador atual deve ter acesso total a esses sites.
- Após a configuração:
    - No console do **Studio**

    - Se você for um administrador de site primário (administrador personalizado ou com acesso total), poderá visualizar os sites secundários na lista suspensa de sites no canto superior direito do console do Studio após acessar o site primário. A lista inclui sites secundários onde você é um administrador com **acesso ao console DaaS**.

  - No console do **Monitor**

    - O gerenciamento de vários sites está disponível apenas para administradores com a função de **Administrador de Help Desk** ou **Administrador de Monitoramento Completo**.

Limitações

- **Limite para quatro sites secundários.** Para um desempenho ideal na agregação de recursos de usuário final por meio de uma única URL de loja, recomendamos adicionar no máximo quatro sites secundários. Por exemplo, exceder esse limite pode levar a logins lentos no Monitor.
- **Grupos de administradores do Microsoft Entra ID (Azure AD).** Para que os grupos de administradores do Microsoft Entra ID funcionem corretamente com o gerenciamento de vários sites, permita que os membros do grupo Entra ID alternem entre as contas do Citrix Cloud. Para fazer isso, vincule as contas entre as quais você deseja que os administradores alternem. Para obter mais informações sobre os grupos de administradores do Microsoft Entra ID (Azure AD), consulte Gerenciar grupos de administradores.

Nota:

- Depois de vincular as contas usando a abordagem baseada em script, a página **Adicionar Sites DaaS** assume como padrão a opção **Adicionar sites DaaS e agregar recursos de usuário final por meio de uma única URL de loja**. Não mude para a opção **Adicionar sites DaaS apenas**. Fazer isso desvinculará as contas, revertendo o link da conta que foi criado usando o script. Como resultado, o gerenciamento de vários sites não funcionará como esperado.
- O gerenciamento de vários sites exige que o grupo de administradores do Entra ID tenha acesso total.

Práticas recomendadas para gerenciamento de vários sites

Para garantir uma experiência consistente de gerenciamento de vários sites, recomendamos fortemente configurar o recurso da seguinte forma:

1. Defina a estrutura da conta.
    a. Identifique uma conta de nuvem primária (hub).
    b. Identifique contas de nuvem secundárias (spokes) para vincular.
2. (Necessário apenas para grupos de administradores do Microsoft Entra ID) Vincule as contas primárias e secundárias.

    Para obter mais informações, consulte Vinculando as contas usando a abordagem baseada em script.
3. Configure o gerenciamento de vários sites.

    Acesso necessário: Administrador com **acesso total** aos sites primário e secundário.

    a. Faça login no **Citrix Cloud** e selecione a *conta primária* na lista de contas.
    b. Na console de gerenciamento do DaaS (Studio), vá para **Configurações > Configurações do site** e clique em **Adicionar** no bloco **Gerenciamento centralizado de sites**.
    c. Selecione os sites secundários. Para obter mais informações, consulte Configurar o gerenciamento centralizado de sites.

    Após a conclusão da configuração, uma lista suspensa de sites aparece no canto superior direito dos consoles Studio e Monitor.
4. Gerenciar um site secundário.

    Acesso necessário: Administrador com acesso total ou personalizado aos sites primário e secundário.

    a. Faça login no **Citrix Cloud** e selecione a *conta primária* na lista de contas.
    b. Acesse um site secundário usando a lista suspensa de sites.
    c. Gerencie este site usando o menu de navegação esquerdo.

Administradores com acesso total: Configurar o gerenciamento centralizado de sites

Como administrador com **acesso total** a vários sites, você pode configurar o gerenciamento centralizado de sites para esses sites.

Preparação

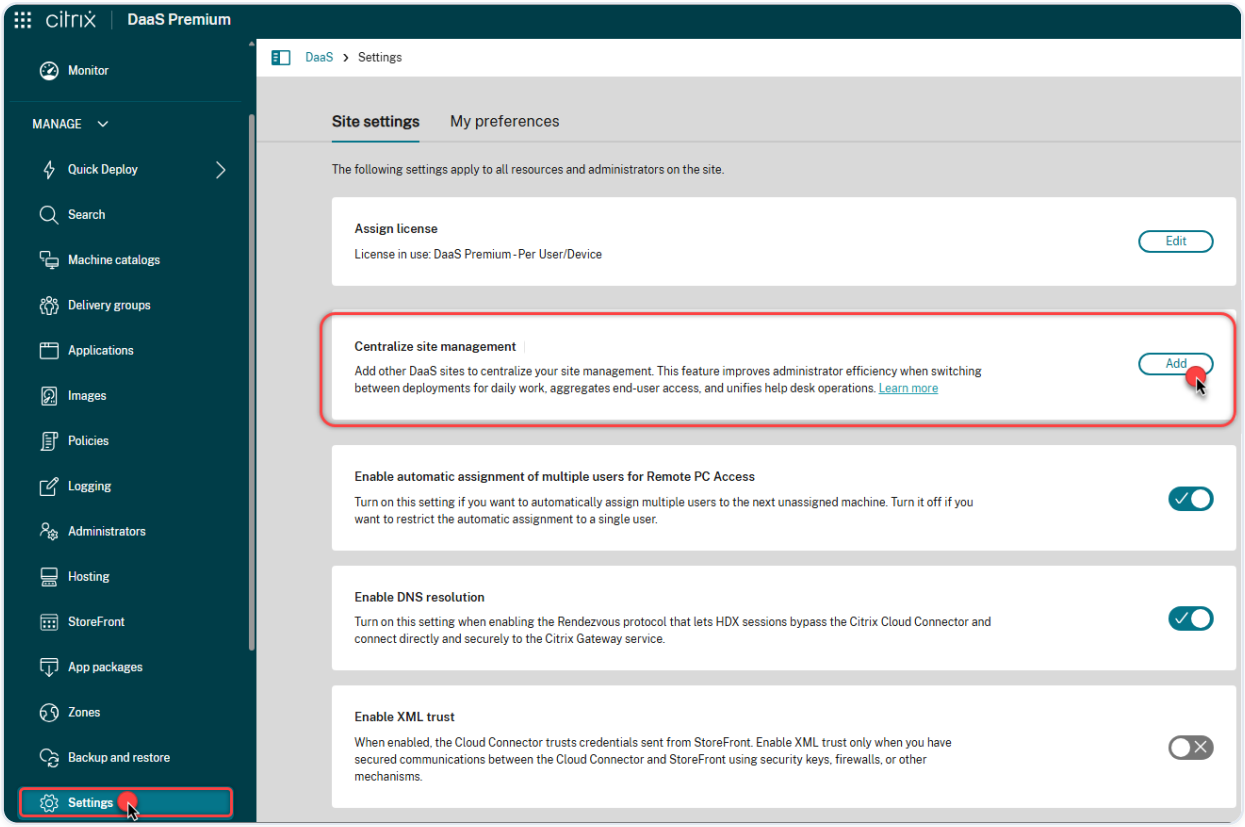
Antes de começar, você precisa:

- **Designar uma conta de nuvem primária**. Determine uma conta de nuvem (também chamada de *site*) onde você gerencia centralmente os sites em sua organização.
- **Certifique-se de ter acesso total**. Certifique-se de ter acesso total a todos os sites que deseja vincular para gerenciamento centralizado. Para obter mais informações, consulte Adicionar um administrador.

Configurar o gerenciamento centralizado de sites

Para configurar o gerenciamento centralizado do site, siga estas etapas:

1. Faça login no **Citrix Cloud™** e selecione a conta da nuvem que você deseja designar como o site *principal*.
2. Acesse **DaaS** para abrir o Studio.
3. No painel esquerdo, selecione **Configurações**.
4. Na guia **Configurações do site**, clique em **Adicionar** no bloco **Gerenciamento centralizado do site**.



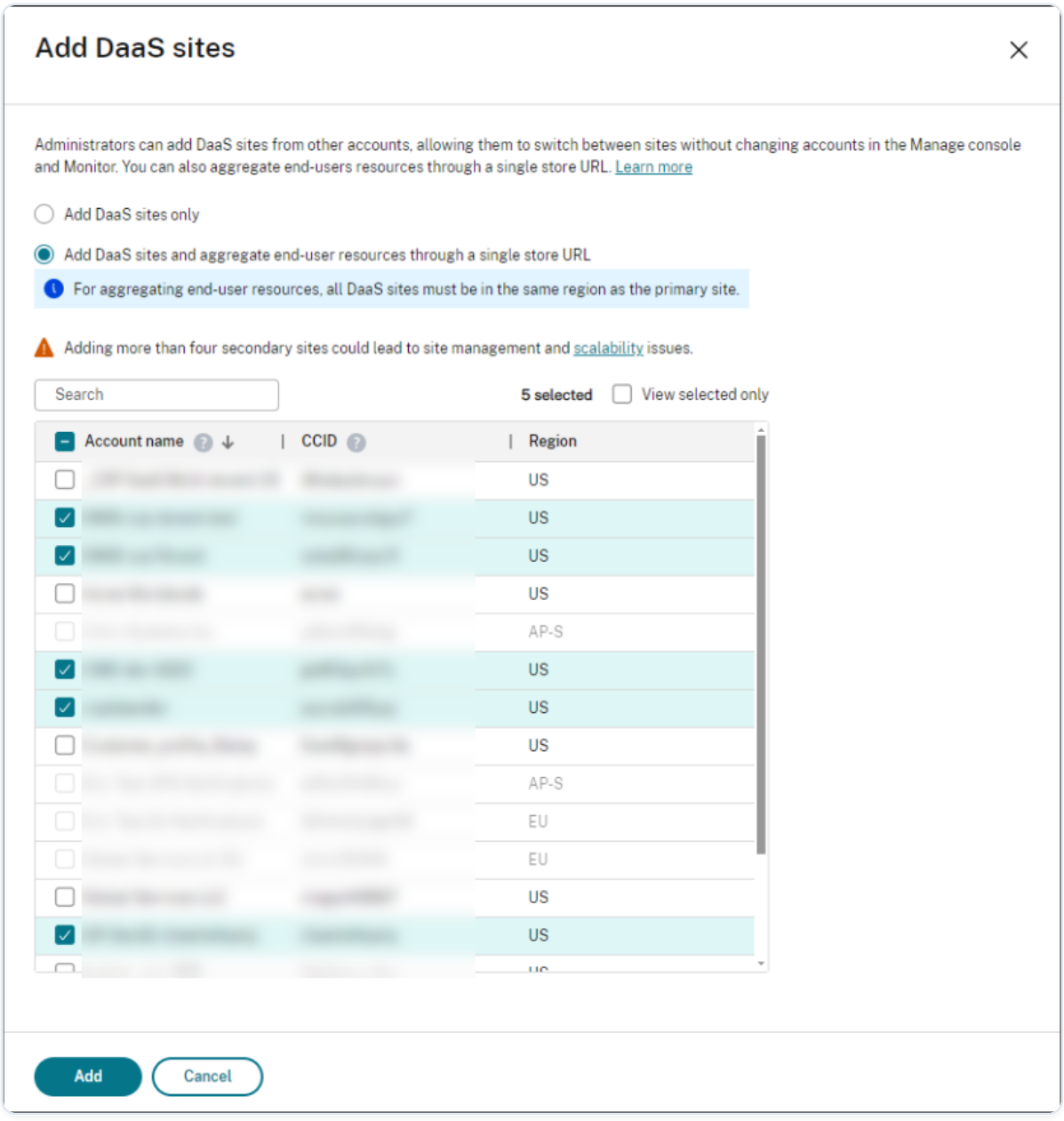
5. Na página **Reconhecer** que aparece, selecione a caixa de seleção de confirmação e clique em **Confirmar** para confirmar a configuração deste site como o principal.

6. Na página **Adicionar sites DaaS** que aparece, preencha as seguintes configurações:

   a. Selecione como você deseja aplicar o gerenciamento centralizado:

      - **Adicionar apenas sites DaaS**. Aplique o gerenciamento centralizado apenas aos consoles Studio e Monitor.
      - **Adicionar sites DaaS e agregar recursos de usuário final por meio de uma única URL de loja**. Aplique o gerenciamento centralizado aos consoles Studio e Monitor e à URL da loja.

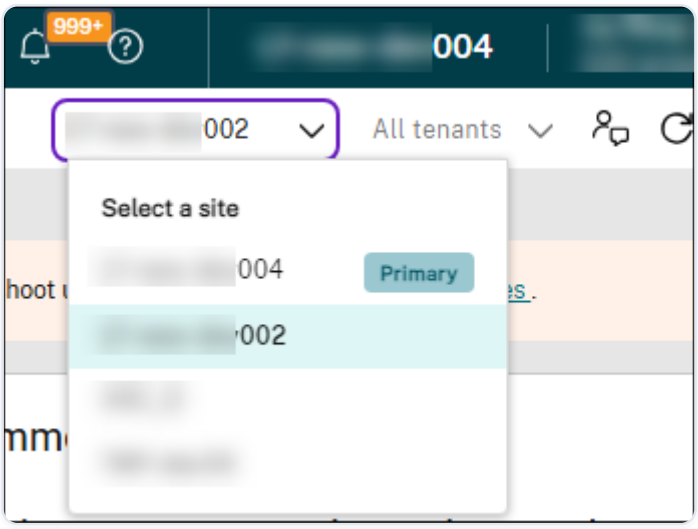
   b. Selecione as contas da nuvem que você deseja adicionar como sites secundários. Apenas as contas da nuvem às quais você tem **acesso total** aparecem.



> **Nota:**
>
> Se você escolheu **Adicionar sites DaaS e agregar recursos de usuário final por meio de uma única URL de loja** na etapa anterior:
>
> - Para um desempenho ideal na agregação de recursos de usuário final, recomendamos adicionar no máximo quatro sites secundários.
> - Apenas os sites localizados na mesma região que o site primário estão disponíveis para seleção como sites secundários.

c. Clique em **Adicionar**.

7. Atualize seu navegador. A caixa de seleção de site aparece no canto superior direito do console, onde este site e seus sites secundários são exibidos.



> **Nota**
>
> - Após a configuração, o gerenciamento de vários sites está disponível para administradores do site primário designado, permitindo que eles gerenciem sites secundários a partir de uma única interface do Studio sem trocar de conta. Para obter mais informações, consulte gerenciar vários sites a partir de uma única interface do Studio.
> - Você também pode habilitar o gerenciamento de vários sites para outros sites na agregação, designando esse site como um site primário.

- O gerenciamento centralizado de sites não é suportado para CSPs e seus locatários, mesmo que o botão **Adicionar** ou **Gerenciar** no bloco **GERENCIAR > Configurações > Gerenciamento centralizado de sites** esteja habilitado.

Adicionar ou remover um site secundário

Como administrador com **acesso total** ao site primário, você pode adicionar ou remover um site secundário do gerenciamento centralizado de sites. As etapas detalhadas são as seguintes:

1. Faça login no Citrix Cloud e selecione o nome da conta do *site primário*.
2. Acesse **DaaS** para abrir o Studio.
3. No painel esquerdo, selecione **Configurações**.
4. No bloco **Gerenciamento centralizado de sites**, clique em **Gerenciar**.
5. Na página **Gerenciar sites DaaS** que aparece, desmarque a caixa de seleção ao lado da conta que você deseja desvincular do site primário ou selecione aquela que você deseja adicionar ao site primário.
6. Clique em **Salvar**.

Nota:

Ao alternar para um site *secundário* através do site *primário*, o botão **Gerenciar** no bloco **GERENCIAR > Configurações > Gerenciamento centralizado de sites** é desativado.

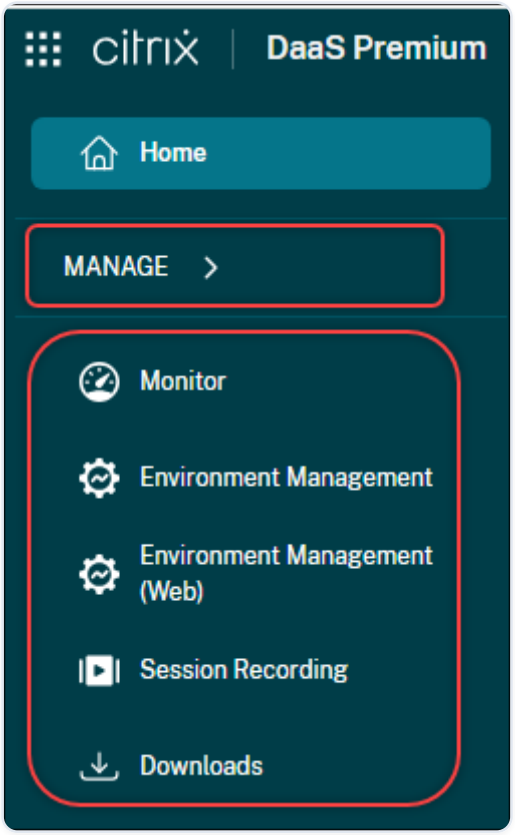
Administradores: Gerencie sites a partir de uma única interface

Após a configuração, como administrador (personalizado ou com acesso total) de vários sites, você pode gerenciá-los a partir de *uma* única interface de usuário do Studio, eliminando a necessidade de trocar de conta.

Considerações ao alternar entre sites

- A configuração de cada site é gerenciada separadamente. As configurações de um site não se mesclam com as de outro no menu **Gerenciar**.
- Quando você está em um site *secundário* a partir do site *primário*:
  - Seu acesso aos itens de menu no menu **GERENCIAR** depende das suas permissões para o site *secundário*.

- Seu acesso aos itens de menu *diferentes de* **GERENCIAR** no painel esquerdo depende das suas permissões para o site *primário*.



Gerenciar sites

Para gerenciar sites a partir de uma única interface, siga estas etapas:

1. Faça login no Citrix Cloud e selecione o nome da conta do site *primário*.
2. Acesse **DaaS** para abrir o Studio.
3. Selecione um site conforme necessário na lista suspensa de sites no canto superior direito. A lista suspensa inclui o site principal e quaisquer sites secundários onde você tenha uma função de administrador com **acesso ao console DaaS**.
4. No painel esquerdo, selecione um nó em **Gerenciar** e inicie seu gerenciamento. *Por exemplo*, selecione **Catálogos de Máquinas** para começar a criar ou gerenciar catálogos para o site selecionado.

Administradores: Monitore sites a partir de uma única interface

Após a configuração, como Administrador de Help Desk ou Administrador de Monitoramento Completo de vários sites, você pode monitorá-los a partir de *uma* única interface de usuário do Monitor, eliminando a necessidade de trocar de conta.

Casos de uso típicos

O gerenciamento centralizado de sites ajuda as organizações a simplificar a administração e o acesso do usuário em vários sites Citrix DaaS™. Esta seção descreve casos de uso comuns.

Administração eficiente de sites

O gerenciamento de vários sites simplifica a administração. Por exemplo, uma organização com três sites DaaS pode gerenciá-los centralmente:

- Site A: Desenvolvimento
- Site B: Teste de Aceitação do Usuário
- Site C: Produção

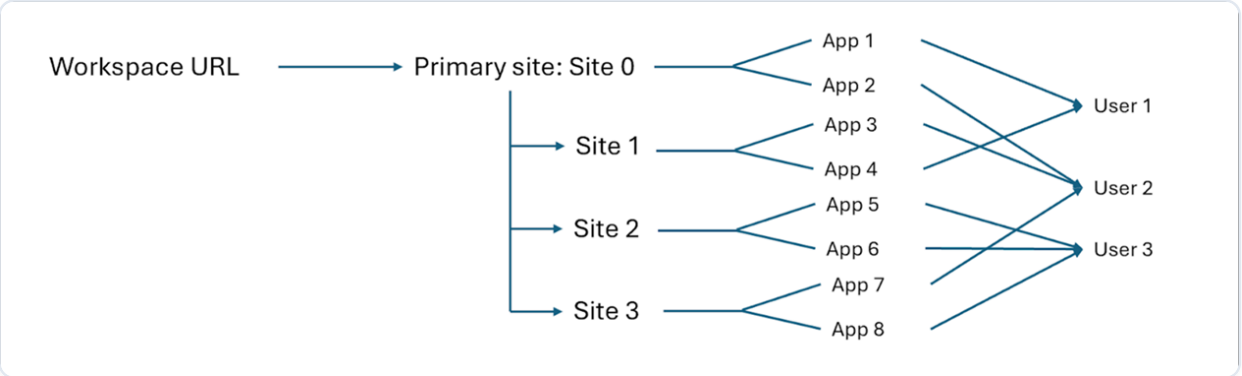
Fusões e aquisições

A aquisição de uma nova empresa geralmente resulta em uma estrutura de domínio complexa, como vários domínios FQDN de florestas diferentes com o mesmo nome em uma relação de confiança de domínio. Um único site pode causar problemas de enumeração de recursos ou de acesso. O gerenciamento de vários sites permite que as organizações mantenham implantações separadas enquanto as gerenciam a partir de uma única interface.

Agregação de recursos do usuário final

Com a agregação de recursos de usuário final ativada, os usuários podem acessar aplicativos e desktops de vários sites através da URL da loja do site principal. Por exemplo:

- Sem agregação: O Usuário 2 deve usar URLs separadas para cada site:
  - URL da loja do Site 0 para acessar o Aplicativo 2
  - URL da loja do Site 1 para acessar o Aplicativo 3
  - URL da loja do Site 3 para acessar o Aplicativo 7
- Com agregação: O Usuário 2 acessa todos os aplicativos através da URL da loja do site principal.



Gerenciar preferências pessoais no Studio

Use a guia **Minhas preferências** no nó **Configurações** para gerenciar suas preferências pessoais de exibição e interação no Studio. Essas configurações se aplicam apenas à sua conta e não afetam outros administradores. As opções disponíveis incluem:

- **Data e hora**: Defina seu fuso horário padrão, formato de data e formato de hora. Essas configurações são usadas em todo o Studio para exibições relacionadas ao tempo, como reinicializações agendadas e dimensionamento automático.
- **Exibição de pasta**: Escolha se deseja mostrar ou ocultar a exibição de pasta nos nós **Catálogos de Máquinas**, **Grupos de Entrega** e **Aplicativos**.
- **Ordem das guias na Pesquisa**: Personalize a ordem das guias dentro do nó **Pesquisa**.

Para definir sua exibição preferida no Studio, siga estas etapas:

1. No Studio, vá para **Configurações > Minhas preferências**.
2. Clique em **Editar**.
3. No bloco **Data e hora**, configure as seguintes configurações de formato:

    - **Formato da data**: Selecione como exibir a data (por exemplo, aaaa/MM/dd). Para usar o formato de data associado ao idioma que você escolheu para o Studio, selecione **Corresponder ao idioma do console**.
    - **Formato da hora:** Selecione um formato de 12 horas (09:00 PM, por exemplo) ou um relógio de 24 horas (21:00, por exemplo). Para usar o formato de hora associado ao idioma que você escolheu para o Studio, selecione **Corresponder ao idioma do console**.
    - **Fuso horário:** Selecione seu fuso horário preferido. Para usar o fuso horário do seu computador, selecione **Corresponder ao idioma do console**.

    > **Nota:**

- Para usar as configurações regionais do seu computador para data, hora ou fuso horário, selecione **Corresponder ao idioma do console**.
- No Studio, você pode passar o mouse sobre qualquer hora exibida para ver seu equivalente em seu fuso horário local.

4. No bloco **Visualização de pasta**, selecione se deseja mostrar ou ocultar a visualização de pasta nos nós **Catálogos de Máquinas**, **Grupos de Entrega** e **Aplicativos**.
5. No bloco **Ordem das guias na Pesquisa**, arraste e reordene as guias dentro do nó **Pesquisa**.
6. Clique em **Aplicar** para salvar e aplicar as alterações imediatamente.

Chaves de segurança

Nota:

- Você deve usar este recurso em combinação com o StoreFront™ 1912 LTSR CU2 ou posterior.
- O recurso Secure XML é compatível apenas com o Citrix ADC e o Citrix Gateway versão 12.1 ou posterior.

Este recurso permite que apenas máquinas StoreFront e Citrix Gateway aprovadas se comuniquem com os Citrix Delivery Controllers. Depois de habilitar este recurso, todas as solicitações que não contiverem a chave serão bloqueadas. Use este recurso para adicionar uma camada extra de segurança para proteger contra ataques originados da rede interna.

Um fluxo de trabalho geral para usar este recurso é o seguinte:

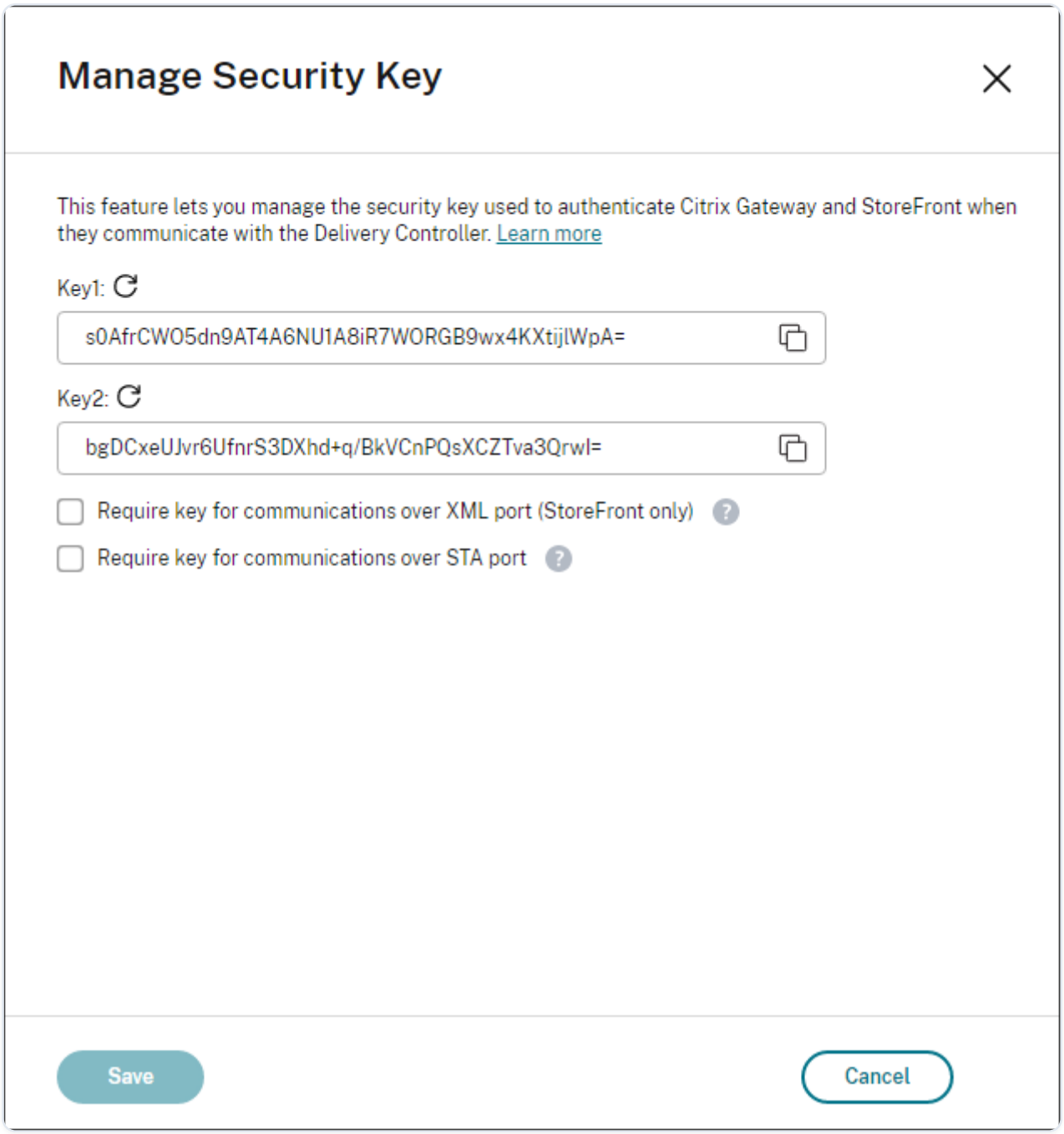
1. Exibir as configurações da chave de segurança no Studio. (Use o SDK do PowerShell Remoto)
2. Configure as configurações para sua implantação. (Use o Studio ou o SDK do PowerShell Remoto).
3. Configure as configurações no StoreFront. (Use o PowerShell).
4. Configure as configurações no Citrix ADC.

Configurar as configurações para sua implantação

Você pode configurar as configurações para sua implantação usando o Studio ou o PowerShell.

Usar o Studio

Após habilitar o recurso, navegar para **Configurações > Configurações do site > Gerenciar chave de segurança** e clique em **Editar**. A lâmina **Gerenciar Chave de Segurança** é exibida. Clique em **Salvar** para aplicar suas alterações e sair da lâmina.



Importante:

> - Existem duas chaves disponíveis para uso. Você pode usar a mesma chave ou chaves diferentes para comunicações pelas portas XML e STA. Recomendamos que você use apenas uma chave por vez. A chave não utilizada é usada apenas para rotação de chaves.
> - Não clique no ícone de atualização para atualizar a chave já em uso. Se o fizer, ocorrerá interrupção do serviço.

> Clique no ícone de atualização para gerar novas chaves.

Exigir chave para comunicações pela porta XML (somente StoreFront). Se selecionado, exige uma chave para autenticar comunicações pela porta XML. O StoreFront se comunica com o Citrix Cloud por esta porta. Para obter informações sobre como alterar a porta XML, consulte o artigo da Central de Conhecimento CTX127945.

Exigir chave para comunicações pela porta STA. Se selecionado, exige uma chave para autenticar comunicações pela porta STA. O Citrix Gateway e o StoreFront se comunicam com o Citrix Cloud por esta porta. Para obter informações sobre como alterar a porta STA, consulte o artigo da Central de Conhecimento CTX101988.

Após aplicar suas alterações, clique em **Fechar** para sair do painel **Gerenciar Chave de Segurança**.

Usar o SDK do PowerShell Remoto

A seguir estão as etapas do PowerShell equivalentes às operações realizadas no Studio.

1. Execute o SDK do PowerShell Remoto.
2. Em uma janela de comando, execute o seguinte comando:
   - `Add-PSSnapIn Citrix*`
3. Execute os seguintes comandos para gerar uma chave e configurar a Chave1:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Execute os seguintes comandos para gerar uma chave e configurar a Chave2:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`

5. Execute um ou ambos os comandos a seguir para habilitar o uso de uma chave na autenticação de comunicações:
    - Para autenticar comunicações pela porta XML:
        - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
    - Para autenticar comunicações pela porta STA:
        - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Consulte a ajuda do comando PowerShell para obter orientação e sintaxe.

Configurar as definições no StoreFront

Após concluir as definições para a sua implantação, você precisa configurar as definições relevantes no StoreFront usando o PowerShell.

No servidor StoreFront, execute os seguintes comandos PowerShell:

Para configurar a chave para comunicações pela porta XML, use o comando Set-STFStoreFarm. Por exemplo:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

Insira os valores apropriados para os seguintes parâmetros:

- `Path to store`
- `Resource feed name`
- `secret`

Para configurar a chave para comunicações sobre a porta STA, use os comandos `New-STFSecureTicketAuthority` e `Set-STFRoamingGateway`. Por exemplo:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

Insira os valores apropriados para os seguintes parâmetros:

- `Gateway name`
- `STA URL`
- `Secret`

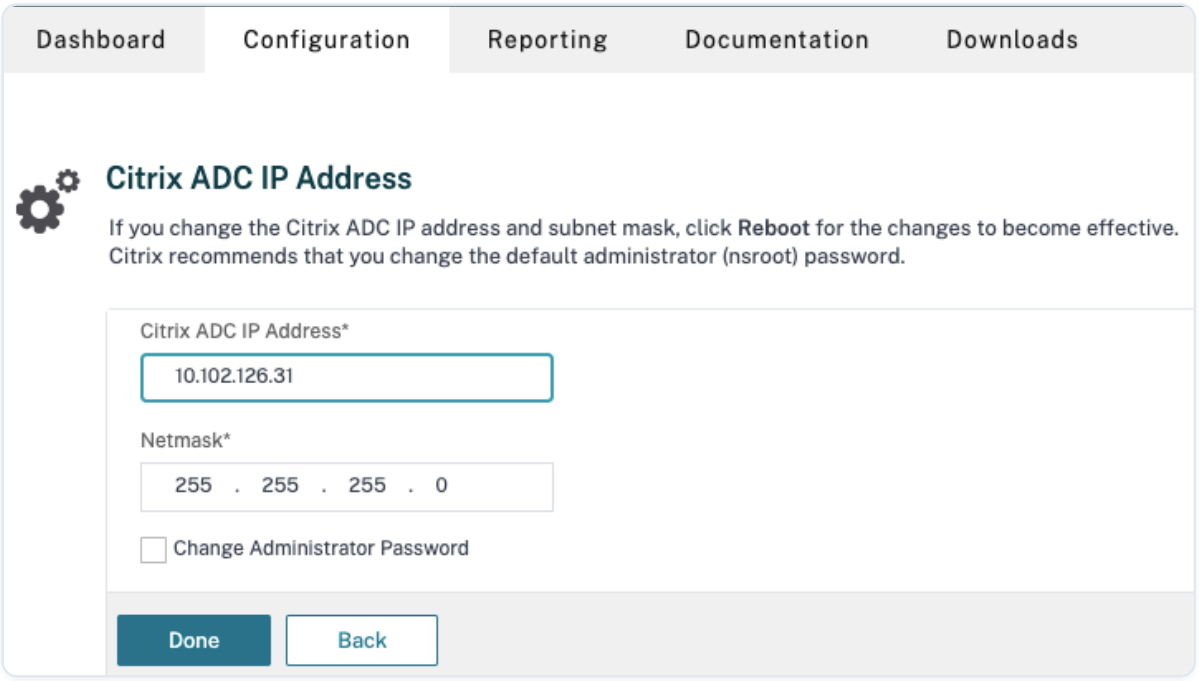
Consulte a ajuda do comando PowerShell para obter orientação e sintaxe.

Configurar definições no Citrix ADC

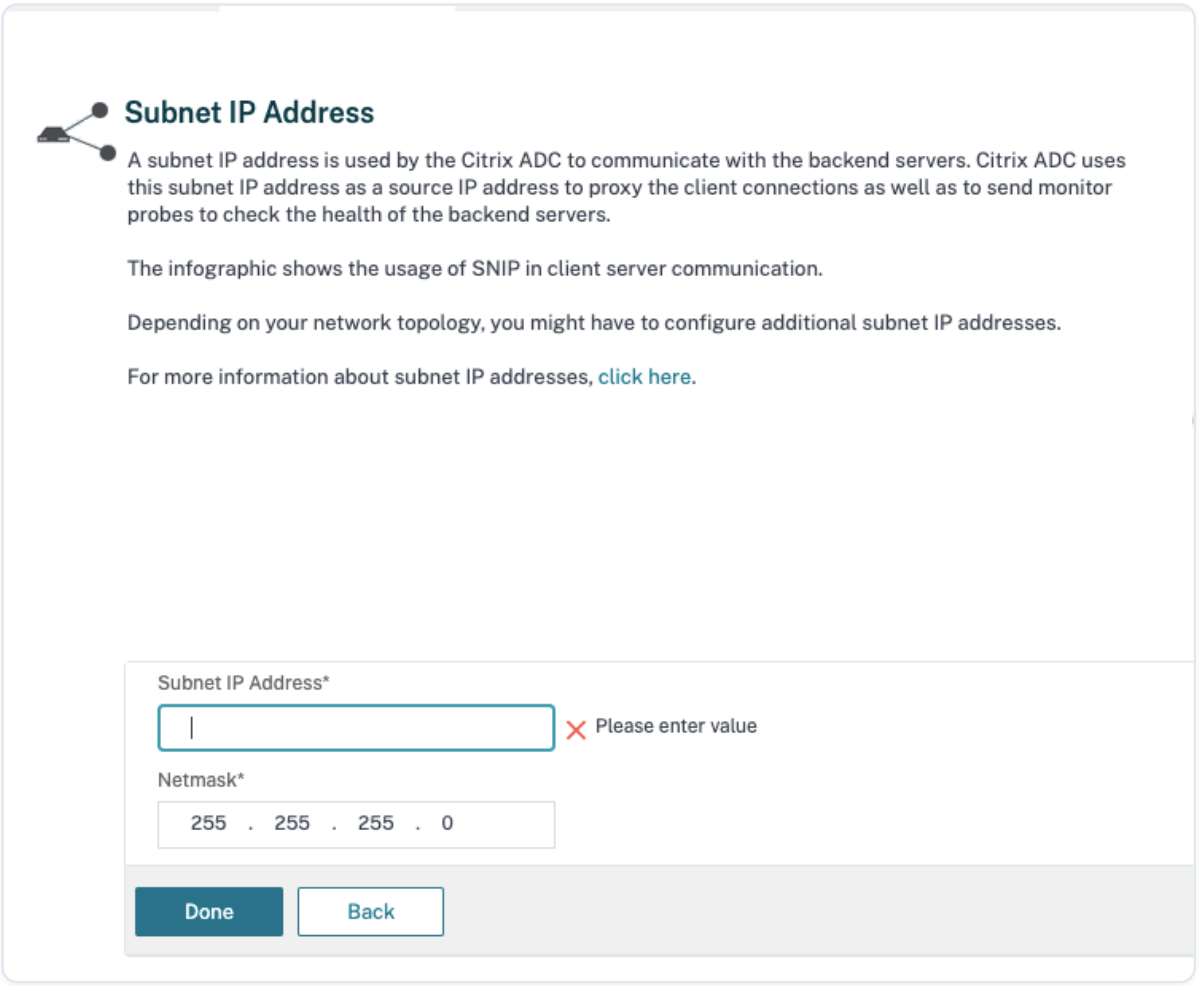
Nota:

A configuração desse recurso no Citrix ADC não é necessária, a menos que você use o Citrix ADC como seu gateway. Se você usar o Citrix ADC, siga as etapas abaixo.

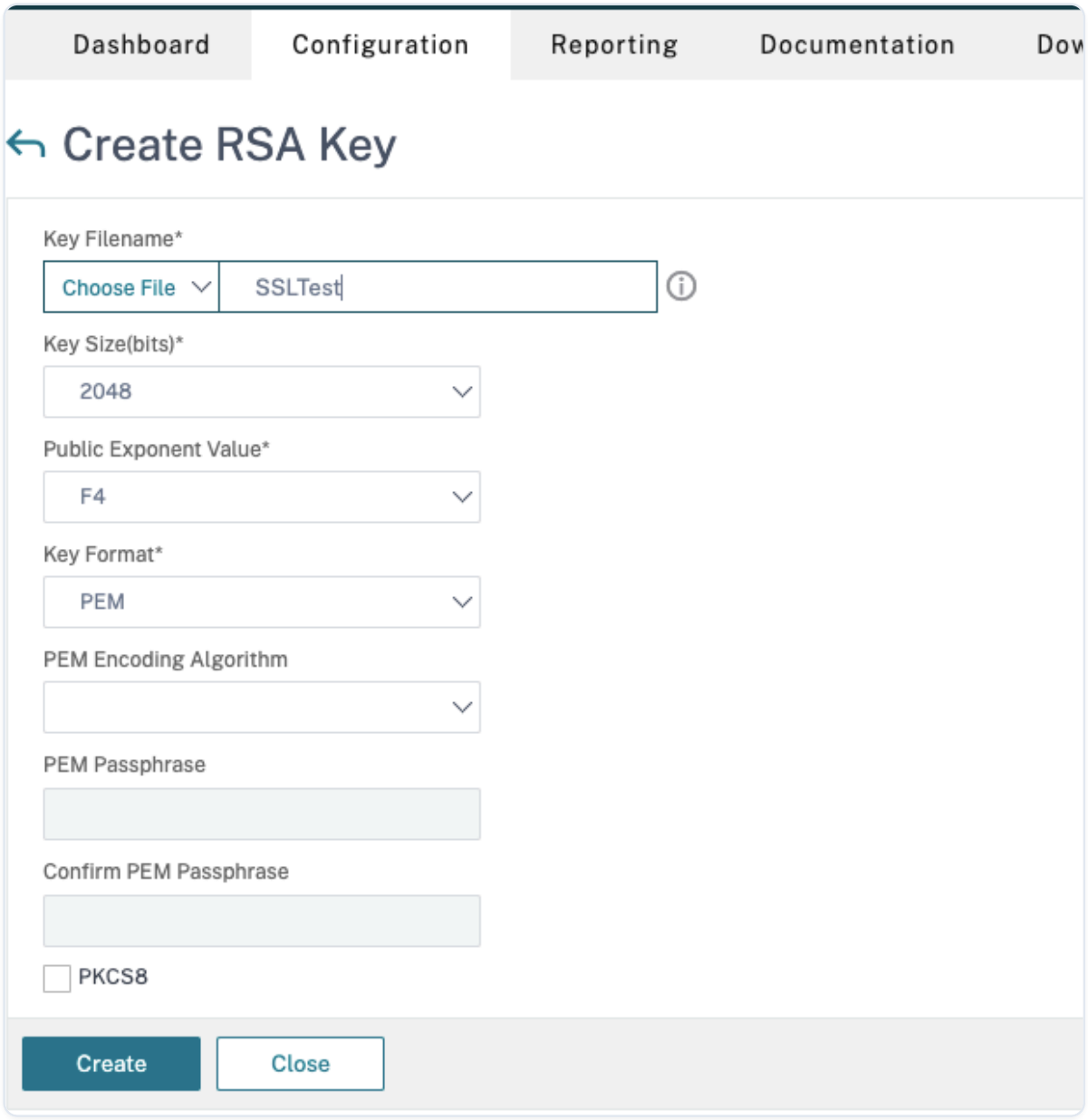
1. Certifique-se de que a seguinte configuração de pré-requisito já esteja em vigor:
    - Os seguintes endereços IP relacionados ao Citrix ADC estão configurados.
        - Endereço IP de Gerenciamento do Citrix ADC (NSIP) para acessar o console do Citrix ADC. Para obter detalhes, consulte Configurando o endereço NSIP.



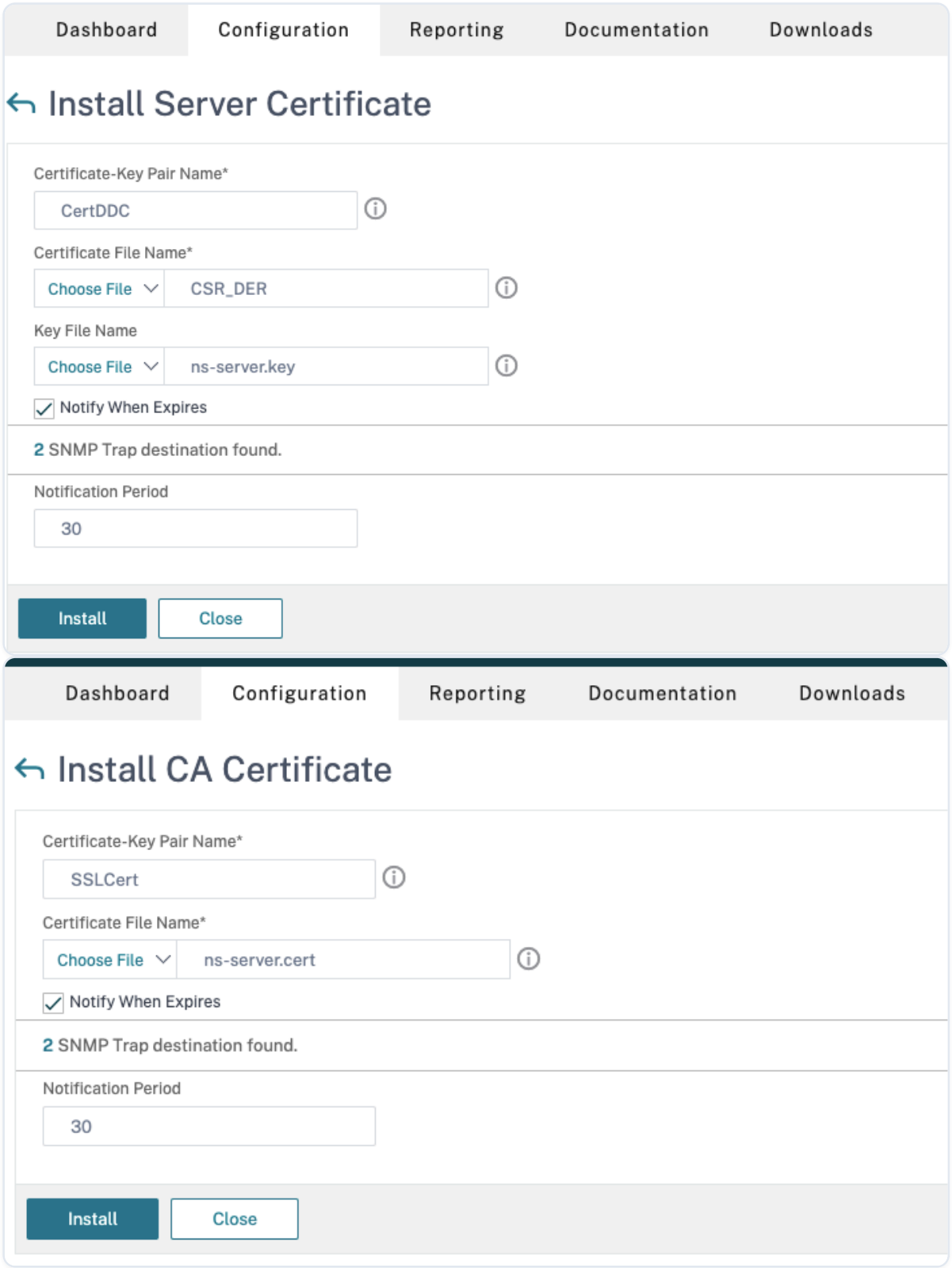
- Endereço IP de sub-rede (SNIP) para habilitar a comunicação entre o dispositivo Citrix ADC e os servidores de back-end. Para obter detalhes, consulte Configuring Subnet IP Addresses.
- Endereço IP virtual do Citrix Gateway e endereço IP virtual do balanceador de carga para fazer login no dispositivo ADC para o lançamento da sessão. Para obter detalhes, consulte Create a virtual server.



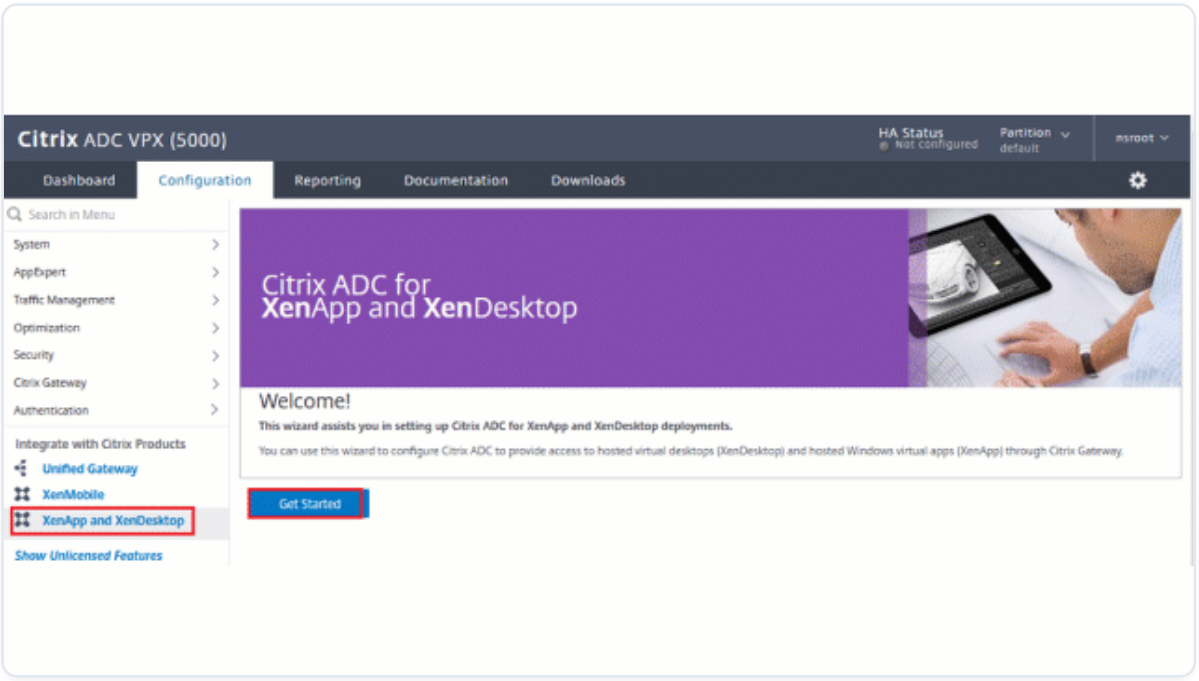
- Os modos e recursos necessários no dispositivo Citrix ADC estão habilitados.
  - Para habilitar os modos, na GUI do Citrix ADC, vá para **System > Settings > Configure Mode**.
  - Para habilitar os recursos, na GUI do Citrix ADC, vá para **System > Settings > Configure Basic Features**.
- As configurações relacionadas a certificados estão concluídas.
  - A Solicitação de Assinatura de Certificado (CSR) é criada. Para obter detalhes, consulte Create a certificate.



- Os certificados de servidor e CA e os certificados raiz são instalados. Para obter detalhes, consulte Install, link, and updates.



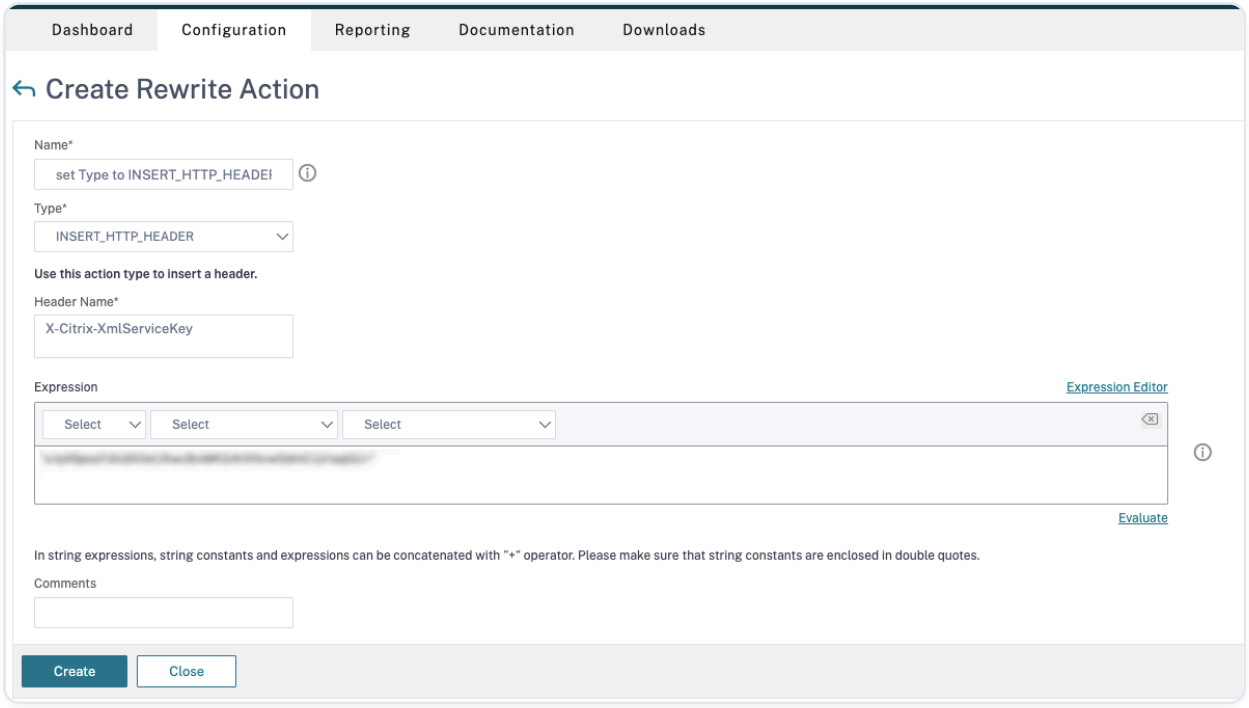
- Um Citrix Gateway foi criado para o Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops). Teste a conectividade clicando no botão **Test STA Connectivity** para confirmar que os servidores virtuais estão online. Para obter detalhes, consulte Setting up Citrix ADC for Citrix Virtual Apps and Desktops.



2. Adicione uma ação de reescrita. Para obter detalhes, consulte Configuring a Rewrite Action.

   a. Vá para **AppExpert > Rewrite > Actions**.

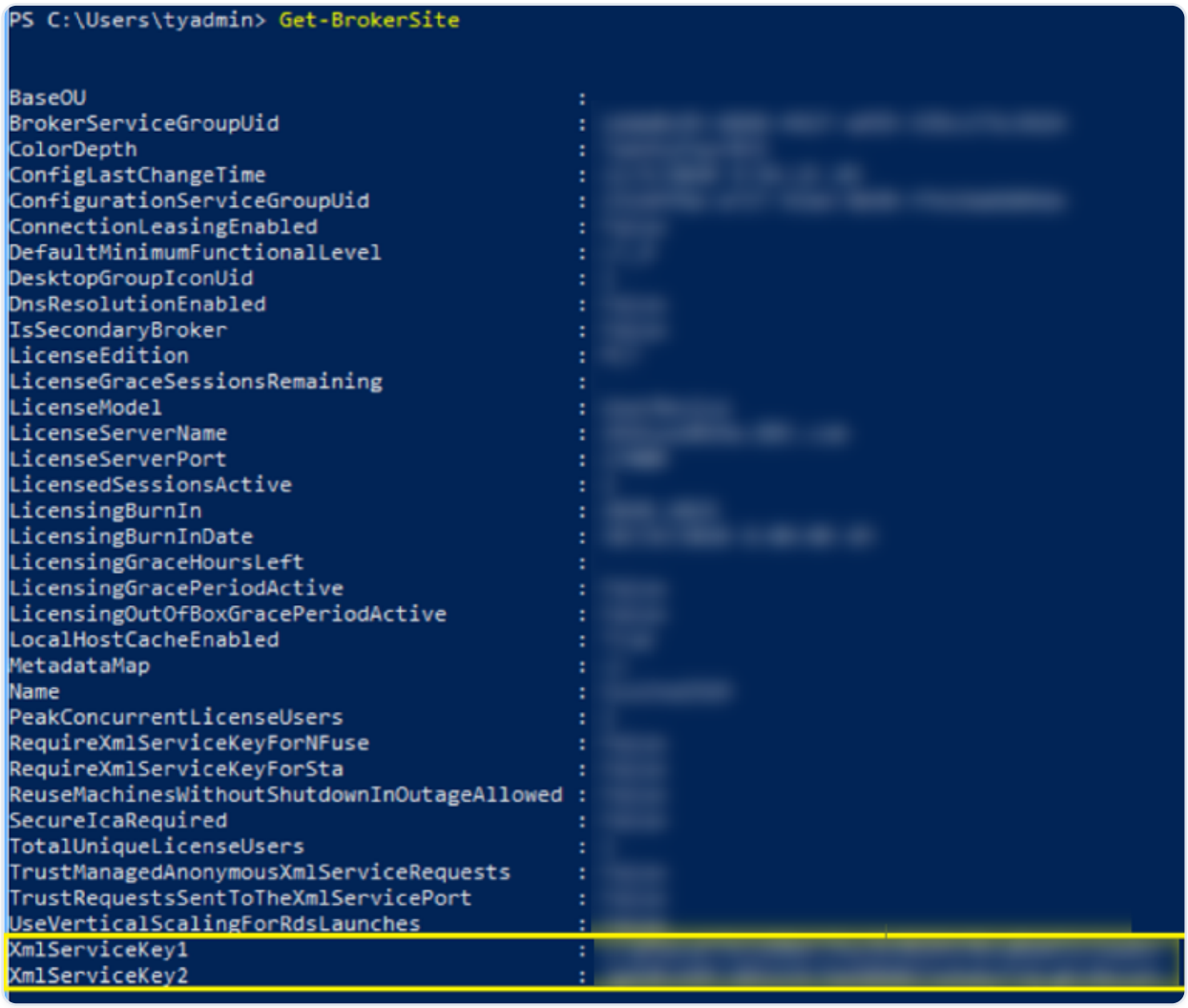
   b. Clique em **Adicionar** para adicionar uma nova ação de reescrita. Você pode nomear a ação como "set Type to INSERT_HTTP_HEADER".



   a. Em **Tipo**, selecione **INSERT_HTTP_HEADER**.

   b. Em **Nome do Cabeçalho**, insira X-Citrix-XmlServiceKey.

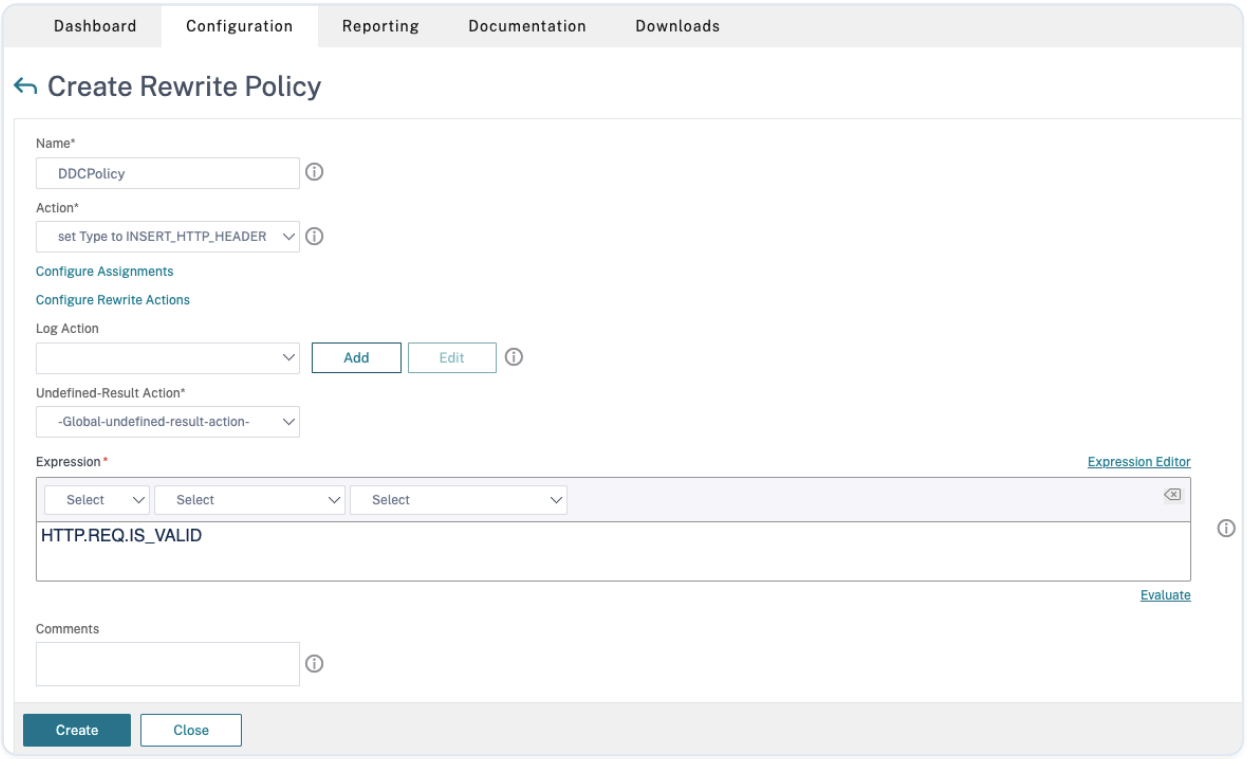
   c. Em **Expressão**, adicione `<XmlServiceKey1 value>` com as aspas. Você pode copiar o valor XmlServiceKey1 da sua configuração do Desktop Delivery Controller™.



3. Adicione uma política de reescrita. Para obter detalhes, consulte Configurando uma Política de Reescrita.

   a. Vá para **AppExpert > Rewrite > Policies**.

   b. Clique em **Adicionar** para adicionar uma nova política.



a. Em **Ação**, selecione a ação criada na etapa anterior.

b. Em **Expressão**, adicione HTTP.REQ.IS_VALID.

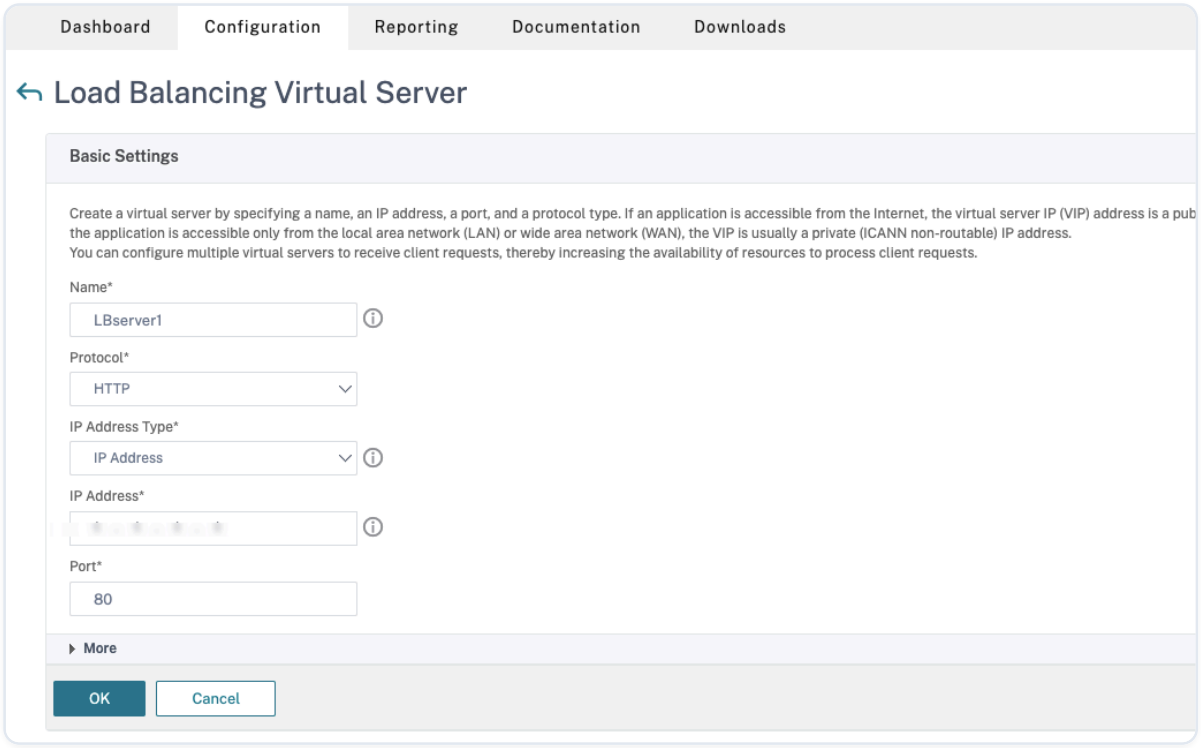
c. Clique em **OK**.

4. Configure o balanceamento de carga. Você deve configurar um servidor virtual de balanceamento de carga por servidor STA. Caso contrário, as sessões não serão iniciadas.

   Para obter detalhes, consulte Configurar balanceamento de carga básico.

   a. Crie um servidor virtual de balanceamento de carga.

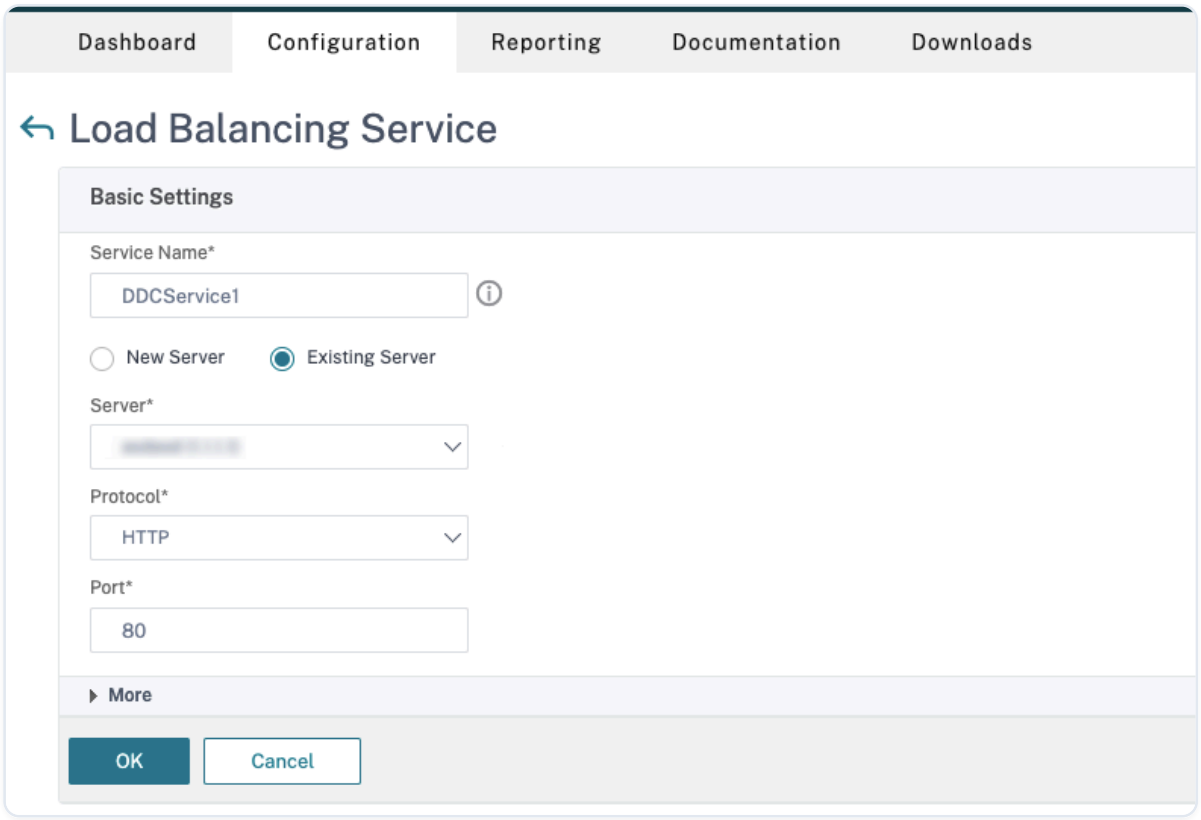
      - Vá para **Gerenciamento de Tráfego > Balanceamento de Carga > Servidores**.
      - Na página **Servidores Virtuais**, clique em **Adicionar**.



- Em **Protocolo**, selecione **HTTP**.
- Adicione o endereço IP virtual de balanceamento de carga e em **Porta** selecione **80**.
- Clique em **OK**.

b. Crie um serviço de balanceamento de carga.

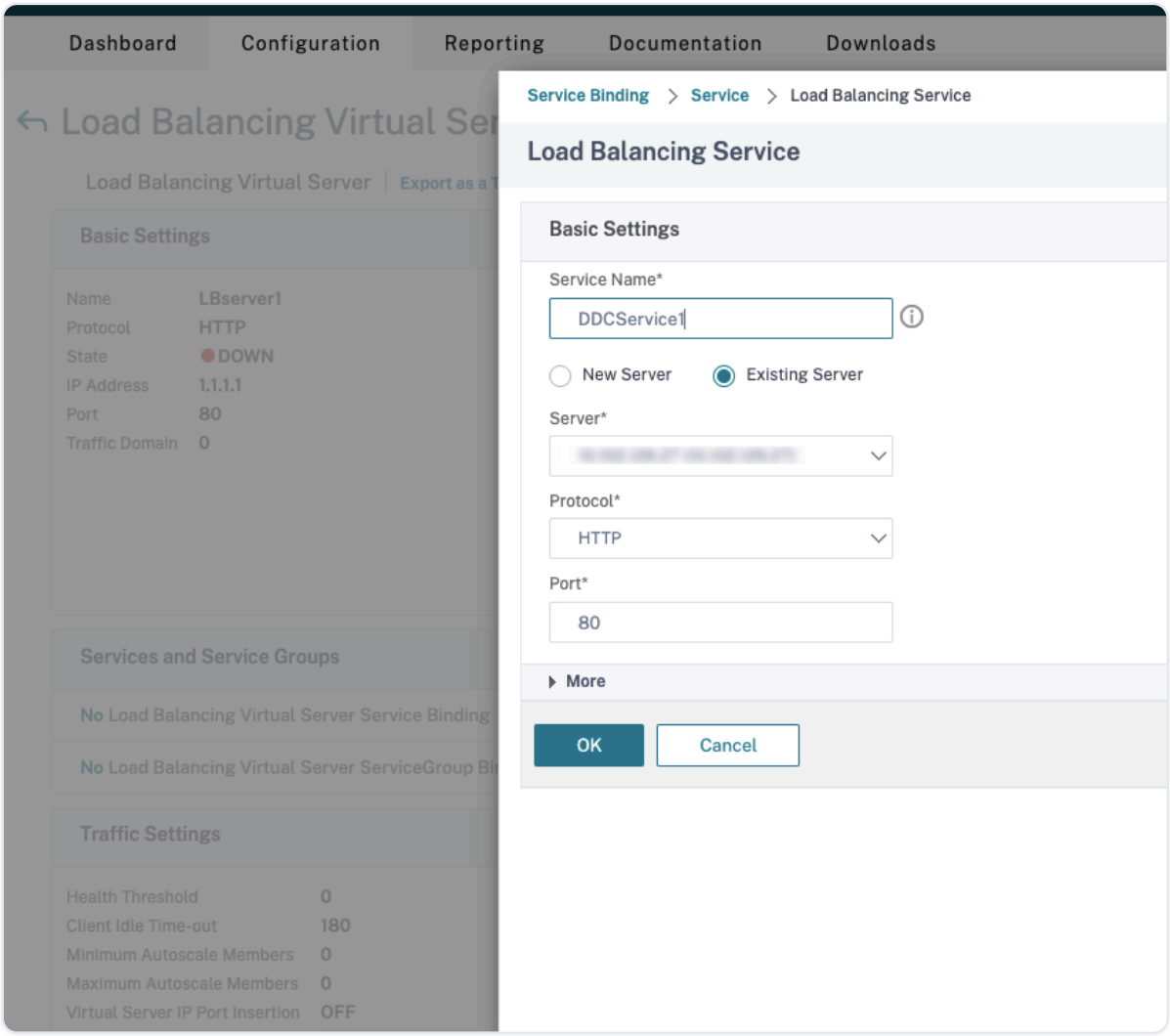
- Vá para **Gerenciamento de Tráfego > Balanceamento de Carga > Serviços**.



- Em **Servidor Existente**, selecione o servidor virtual criado na etapa anterior.
- Em **Protocolo**, selecione **HTTP** e em **Porta** selecione **80**.
- Clique em **OK** e, em seguida, clique em **Concluído**.

c. Vincule o serviço ao servidor virtual.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.
- Em **Serviços e Grupos de Serviço**, clique em **Nenhuma Vinculação de Serviço de Servidor Virtual de Balanceamento de Carga**.

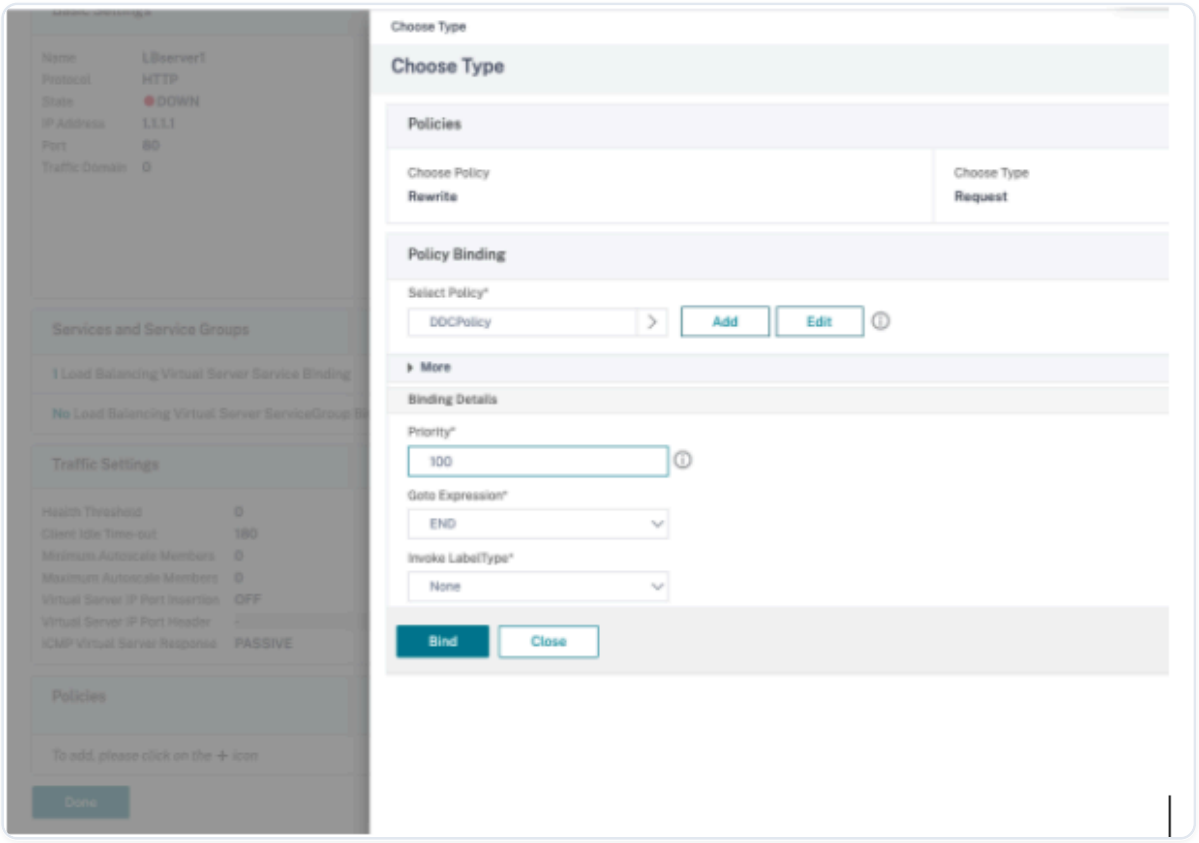


- Em **Vinculação de Serviço**, selecione o Citrix DaaS™ criado anteriormente.
- Clique em **Vincular**.

d. Vincule a política de reescrita criada anteriormente ao servidor virtual.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.

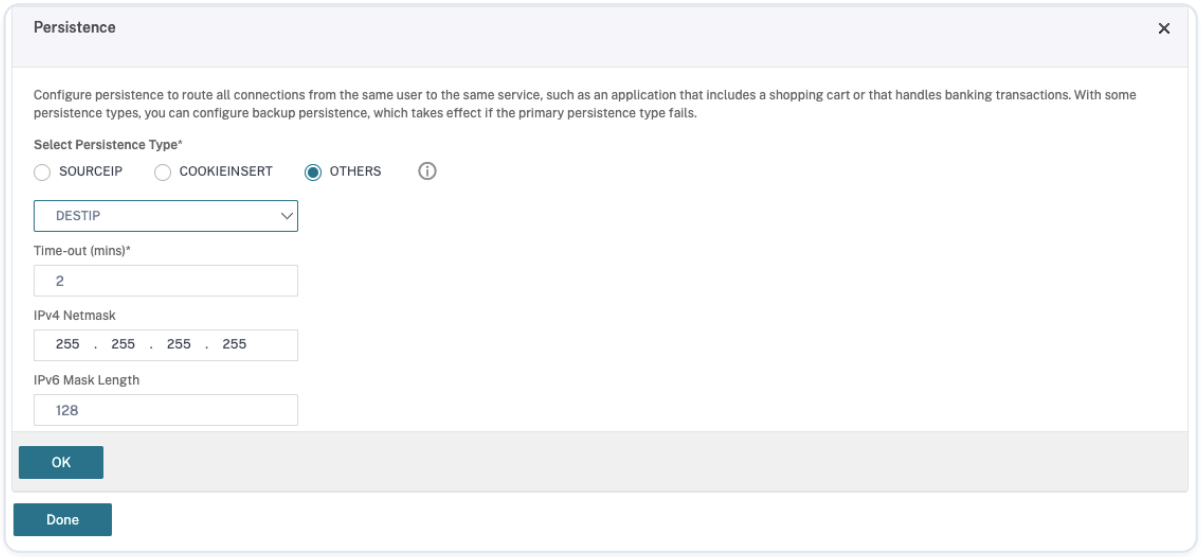
- Em **Configurações Avançadas**, clique em **Políticas,** e, em seguida, na seção **Políticas**, clique em **+**.



- Em **Escolher Política**, selecione **Reescrever** e em **Escolher Tipo**, selecione **Solicitação**.
- Clique em **Continuar**.
- Em **Selecionar Política**, selecione a política de reescrita criada anteriormente.
- Clique em **Vincular**.
- Clique em **Concluído**.

e. Configure a persistência para o servidor virtual, se necessário.

- Selecione o servidor virtual criado anteriormente e clique em **Editar**.
- Em **Configurações Avançadas**, clique em **Persistência**.



- Selecione o tipo de persistência como **Outros**.
- Selecione **DESTIP** para criar sessões de persistência com base no endereço IP do serviço selecionado pelo servidor virtual (o endereço IP de destino)
- Em **Máscara de Rede IPv4**, adicione a máscara de rede igual à do DDC.
- Clique em **OK**.

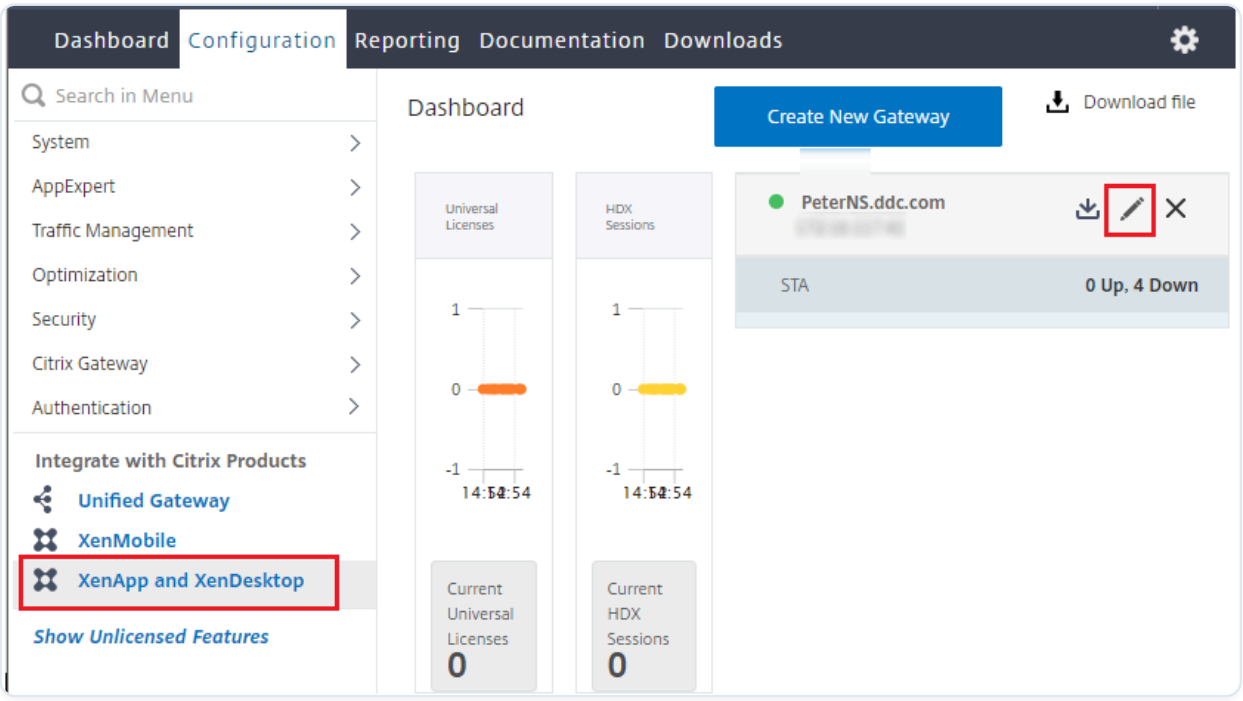
f. Repita estas etapas para o outro servidor virtual também.

Alterações de configuração se o dispositivo Citrix ADC já estiver configurado com o Citrix DaaS

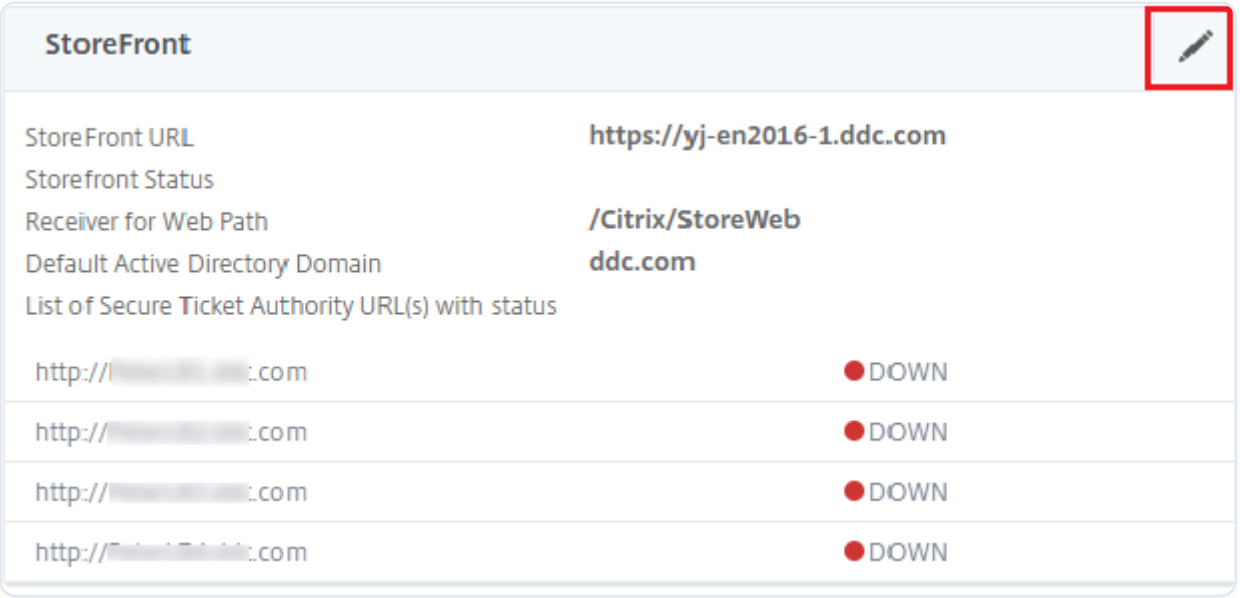
Se você já configurou o dispositivo Citrix ADC com o Citrix DaaS, para usar o recurso Secure XML, você deve fazer as seguintes alterações de configuração.

- Antes do lançamento da sessão, altere a **URL da Autoridade de Ticket de Segurança** do gateway para usar os FQDNs dos servidores virtuais de balanceamento de carga.
- Certifique-se de que o parâmetro `TrustRequestsSentToTheXmlServicePort` esteja definido como Falso. Por padrão, o parâmetro `TrustRequestsSentToTheXmlServicePort` é definido como Falso. No entanto, se o cliente já configurou o Citrix ADC para o Citrix DaaS, então o `TrustRequestsSentToTheXmlServicePort` é definido como Verdadeiro.

1. Na GUI do Citrix ADC, vá para **Configuração > Integrar com Produtos Citrix** e clique em **XenApp and XenDesktop®**.
2. Selecione a instância do gateway e clique no ícone de edição.

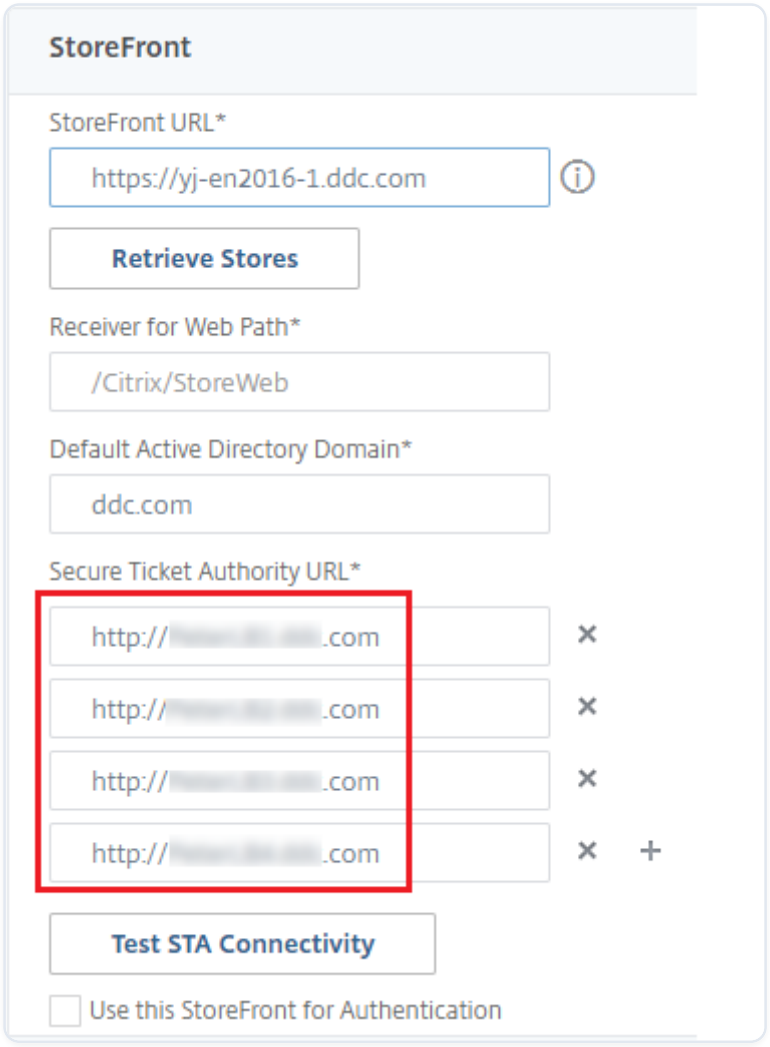


3. No painel StoreFront, clique no ícone de edição.



4. Adicione a **URL da Secure Ticket Authority**.

   - Se o recurso Secure XML estiver ativado, a URL do STA deve ser a URL do serviço de balanceamento de carga.
   - Se o recurso Secure XML estiver desativado, a URL do STA deve ser a URL do STA (endereço do DDC) e o parâmetro TrustRequestsSentToTheXmlServicePort no DDC deve ser definido como True.



Configurações de resiliência de sessão

Manter a atividade da sessão é fundamental para proporcionar a melhor experiência ao usuário. A perda de conectividade devido a redes não confiáveis, latência de rede altamente variável e limitações de alcance de dispositivos sem fio pode levar à frustração do usuário. Ser capaz de se mover rapidamente entre estações de trabalho e acessar o mesmo conjunto de aplicativos cada vez que fazem login é uma prioridade para muitos trabalhadores móveis, como profissionais de saúde em um hospital.

Os recursos descritos neste artigo otimizam a confiabilidade das sessões, reduzem inconvenientes, tempo de inatividade e perda de produtividade; usando esses recursos, os usuários móveis podem se deslocar de forma rápida e fácil entre os dispositivos.

Confiabilidade da sessão

A Confiabilidade da Sessão mantém as sessões ativas e na tela do usuário quando a conectividade de rede é interrompida. Os usuários continuam a ver o aplicativo que estão usando até que a conectividade de rede seja retomada.

Este recurso é especialmente útil para usuários móveis com conexões sem fio. Por exemplo, um usuário com uma conexão sem fio entra em um túnel ferroviário e perde momentaneamente a conectividade. Normalmente, a sessão é desconectada e desaparece da tela do usuário, e o usuário precisa se reconectar à sessão desconectada. Com a Confiabilidade da Sessão, a sessão permanece ativa na máquina. Para indicar que a conectividade foi perdida, a tela do usuário congela e o cursor muda para uma ampulheta giratória até que a conectividade seja retomada do outro lado do túnel. O usuário continua a acessar a exibição durante a interrupção e pode retomar a interação com o aplicativo quando a conexão de rede for restaurada. A Confiabilidade da Sessão reconecta os usuários sem prompts de reautenticação.

Os usuários do aplicativo Citrix Workspace™ não podem substituir a configuração do Controller.

Você pode usar a Confiabilidade da Sessão com o Transport Layer Security (TLS). O TLS criptografa apenas os dados enviados entre o dispositivo do usuário e o Citrix Gateway.

Habilite e configure a Confiabilidade da Sessão com as seguintes configurações de política:

- A configuração de política de conexões de confiabilidade da sessão permite ou impede a confiabilidade da sessão.
- A configuração de política de tempo limite de confiabilidade da sessão tem um padrão de 180 segundos, ou três minutos. Embora você possa estender o tempo que a Confiabilidade da Sessão mantém uma sessão aberta, esse recurso foi projetado para a conveniência do usuário e, portanto, não solicita reautenticação ao usuário. À medida que você estende o tempo em que uma sessão é mantida aberta, aumentam as chances de um usuário se distrair e se afastar do dispositivo do usuário, potencialmente deixando a sessão acessível a usuários não autorizados.
- As conexões de confiabilidade de sessão de entrada usam a porta 2598, a menos que você altere o número da porta na configuração de política de número de porta de confiabilidade da sessão.
- Se você não quiser que os usuários possam se reconectar a sessões interrompidas sem ter que se reautenticar, use o recurso Auto Client Reconnect. Você pode configurar a configuração de política de autenticação de reconexão automática do cliente para solicitar que os usuários se reautentiquem ao se reconectarem a sessões interrompidas.

Se você usar a Confiabilidade da Sessão e o Auto Client Reconnect, os dois recursos funcionarão em sequência. A Confiabilidade da Sessão fecha, ou desconecta, a sessão do usuário após o tempo especificado na configuração de política de tempo limite de confiabilidade da sessão. Depois disso, as configurações de política do Auto Client Reconnect entram em vigor, tentando reconectar o usuário à sessão desconectada.

Auto Client Reconnect

Com o recurso Auto Client Reconnect, o aplicativo Citrix Workspace pode detectar desconexões não intencionais de sessões ICA® e reconectar os usuários às sessões afetadas automaticamente. Quando esse recurso é habilitado no servidor, os usuários não precisam se reconectar manualmente para continuar trabalhando.

Para sessões de aplicativo, o aplicativo Citrix Workspace tenta se reconectar à sessão até que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão.

Para sessões de desktop, o aplicativo Citrix Workspace tenta se reconectar à sessão por um tempo especificado, a menos que haja uma reconexão bem-sucedida ou o usuário cancele as tentativas de reconexão. Por padrão, esse tempo é de cinco minutos. Para alterar esse período, edite este registro no dispositivo do usuário:

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

Onde `seconds` é o número de segundos após os quais nenhuma outra tentativa é feita para reconectar a sessão.

Habilite e configure o Auto Client Reconnect com as seguintes configurações de política:

- **Reconexão automática do cliente:** Habilita ou desabilita a reconexão automática pelo aplicativo Citrix Workspace depois que uma conexão foi interrompida.
- **Autenticação de reconexão automática do cliente:** Habilita ou desabilita a exigência de autenticação do usuário após a reconexão automática.
- **Registro de reconexão automática do cliente:** Habilita ou desabilita o registro de eventos de reconexão no log de eventos. O registro é desabilitado por padrão. Quando habilitado, o Log do Sistema do servidor captura informações sobre eventos de reconexão automática bem-sucedidos e falhos. Cada servidor armazena informações sobre eventos de reconexão em seu próprio log do sistema. O site não fornece um log combinado de eventos de reconexão para todos os servidores.

O Auto Client Reconnect incorpora um mecanismo de autenticação baseado em credenciais de usuário criptografadas. Quando um usuário faz logon inicialmente, o servidor criptografa e armazena as credenciais do usuário na memória, e cria e envia um cookie contendo a chave de criptografia para o aplicativo Citrix Workspace. O aplicativo Citrix Workspace envia a chave para o servidor para reconexão. O servidor descriptografa as credenciais e as envia para o Logon do

Windows para autenticação. Quando os cookies expiram, os usuários devem se reautenticar para se reconectar às sessões.

Os cookies não são usados se você habilitar a configuração de autenticação de reconexão automática do cliente. Em vez disso, uma caixa de diálogo é apresentada aos usuários solicitando credenciais quando o aplicativo Citrix Workspace tenta se reconectar automaticamente.

Para proteção máxima das credenciais e sessões do usuário, use criptografia para toda a comunicação entre clientes e o Site.

Desabilite o Auto Client Reconnect no aplicativo Citrix Workspace para Windows usando o arquivo icaclient.adm. Para obter mais informações, consulte a documentação da sua versão do aplicativo Citrix Workspace para Windows.

As configurações para conexões também afetam o Auto Client Reconnect:

- Por padrão, o Auto Client Reconnect é habilitado por meio de configurações de política no nível do Site, conforme descrito acima. A reautenticação do usuário não é necessária. No entanto, se a conexão ICA TCP de um servidor estiver configurada para redefinir sessões com um link de comunicação interrompido, a reconexão automática não ocorrerá. O Auto Client Reconnect funciona somente se o servidor desconectar as sessões quando houver uma conexão interrompida ou com tempo limite esgotado. Nesse contexto, a conexão ICA TCP refere-se a uma porta virtual do servidor (em vez de uma conexão de rede real) que é usada para sessões em redes TCP/IP.
- Por padrão, a conexão TCP ICA em um servidor é configurada para desconectar sessões com conexões quebradas ou expiradas. As sessões desconectadas permanecem intactas na memória do sistema e estão disponíveis para reconexão pelo Citrix Workspace app.
- A conexão pode ser configurada para redefinir ou desconectar sessões com conexões quebradas ou expiradas. Quando uma sessão é redefinida, a tentativa de reconexão inicia uma nova sessão. Em vez de restaurar o usuário para o mesmo ponto no aplicativo em uso, o aplicativo é reiniciado.
- Se o servidor estiver configurado para redefinir sessões, o Auto Client Reconnect criará uma sessão. Esse processo exige que os usuários insiram suas credenciais para fazer logon no servidor.
- A reconexão automática pode falhar se o Citrix Workspace app ou o plug-in enviar informações de autenticação incorretas, o que pode ocorrer durante um ataque ou se o servidor determinar que muito tempo se passou desde que detectou a conexão quebrada.

ICA Keep-Alive

A habilitação do recurso ICA Keep-Alive impede que conexões quebradas sejam desconectadas. Quando habilitado, se o servidor não detectar atividade (por exemplo, nenhuma alteração de relógio, nenhum movimento do mouse, nenhuma atualização de tela), esse recurso impede que os Serviços de Área de Trabalho Remota desconectem essa sessão. O servidor envia pacotes keep-alive a cada poucos segundos para detectar se a sessão está ativa. Se a sessão não estiver mais ativa, o servidor a marca como desconectada.

> **Importante:**
>
> O ICA Keep-Alive funciona somente se você não estiver usando a Confiabilidade da Sessão. A Confiabilidade da Sessão tem seus próprios mecanismos para evitar que conexões quebradas sejam desconectadas. Configure o ICA Keep-Alive apenas para conexões que não usam a Confiabilidade da Sessão.

> As configurações do ICA Keep-Alive substituem as configurações de keep-alive configuradas na Política de Grupo do Microsoft Windows.

Habilite e configure o ICA Keep-Alive com as seguintes configurações de política:

- **Tempo limite de keep-alive do ICA:** Especifica o intervalo (1–3600 segundos) usado para enviar mensagens keep-alive do ICA. Não configure esta opção se você quiser que seu software de monitoramento de rede feche conexões inativas em ambientes onde as conexões quebradas são tão infrequentes que permitir que os usuários se reconectem às sessões não é uma preocupação.

  O intervalo padrão é de 60 segundos: pacotes ICA Keep-Alive são enviados aos dispositivos do usuário a cada 60 segundos. Se um dispositivo de usuário não responder em 60 segundos, o status das sessões ICA muda para desconectado.
- **Keep-alives do ICA:** Envia ou impede o envio de mensagens keep-alive do ICA.

Controle de workspace

O controle de workspace permite que desktops e aplicativos sigam um usuário de um dispositivo para outro. Essa capacidade de roaming permite que um usuário acesse todos os desktops ou aplicativos abertos de qualquer lugar simplesmente fazendo logon, sem precisar reiniciar os desktops ou aplicativos em cada dispositivo. Por exemplo, o controle de workspace pode auxiliar profissionais de saúde em um hospital que precisam se mover rapidamente entre diferentes

estações de trabalho e acessar o mesmo conjunto de aplicativos a cada logon. Se você configurar as opções de controle de workspace para permitir, esses trabalhadores podem se desconectar de vários aplicativos em um dispositivo cliente e, em seguida, reconectar-se para abrir os mesmos aplicativos em um dispositivo cliente diferente.

O controle de workspace afeta as seguintes atividades:

- **Fazer logon:** Por padrão, o controle de workspace permite que os usuários se reconectem automaticamente a todos os desktops e aplicativos em execução ao fazer logon, eliminando a necessidade de reabri-los manualmente. Através do controle de workspace, os usuários podem abrir desktops ou aplicativos desconectados, e quaisquer que estejam ativos em outro dispositivo cliente. Desconectar-se de um desktop ou aplicativo o deixa em execução no servidor. Se você tiver usuários itinerantes que precisam manter alguns desktops ou aplicativos em execução em um dispositivo cliente enquanto se reconectam a um subconjunto de seus desktops ou aplicativos em outro dispositivo cliente, você pode configurar o comportamento de reconexão de logon para abrir apenas os desktops ou aplicativos dos quais o usuário se desconectou anteriormente.
- **Reconectando:** Após fazer logon no servidor, os usuários podem se reconectar a todos os seus desktops ou aplicativos a qualquer momento clicando em Reconectar. Por padrão, Reconectar abre desktops ou aplicativos que estão desconectados, além de quaisquer que estejam atualmente em execução em outro dispositivo cliente. Você pode configurar Reconectar para abrir apenas os desktops ou aplicativos dos quais o usuário se desconectou anteriormente.
- **Fazer logoff:** Para usuários que abrem desktops ou aplicativos através do StoreFront™, você pode configurar o comando Fazer Logoff para desconectar o usuário do StoreFront e de todas as sessões ativas juntas, ou desconectar apenas do StoreFront.
- **Desconectando:** Os usuários podem se desconectar de todos os desktops e aplicativos em execução de uma só vez, sem a necessidade de se desconectar de cada um individualmente.

O controle de workspace está disponível para usuários que acessam desktops e aplicativos através de uma conexão Citrix StoreFront ou através do aplicativo Citrix Workspace. Por padrão, o controle de workspace está desabilitado para sessões de desktop virtual, mas está habilitado para aplicativos hospedados. O compartilhamento de sessão não ocorre por padrão entre desktops publicados e quaisquer aplicativos publicados em execução dentro desses desktops.

As políticas de usuário, mapeamentos de unidade cliente e configurações de impressora mudam apropriadamente quando um usuário se move para um novo dispositivo cliente. As políticas e mapeamentos são aplicados de acordo com o dispositivo cliente onde o usuário está logado na

sessão. Por exemplo, se um profissional de saúde faz logoff de um dispositivo cliente na sala de emergência de um hospital e depois faz logon em uma estação de trabalho no laboratório de raios-X do hospital, as políticas, mapeamentos de impressora e mapeamentos de unidade cliente apropriados para a sessão no laboratório de raios-X entram em vigor no início da sessão.

Você pode personalizar quais impressoras aparecem para os usuários quando eles mudam de local. Você também pode controlar se os usuários podem imprimir em impressoras locais, quanta largura de banda é consumida quando os usuários se conectam remotamente e outros aspectos de suas experiências de impressão.

Para obter informações sobre como habilitar e configurar o controle de workspace para usuários, consulte a documentação do StoreFront.

Roaming de sessão

> **Nota:**
>
> As informações a seguir o guiam para configurar o roaming de sessão usando o PowerShell. Você pode usar o Studio em vez disso. Para obter mais informações, consulte Gerenciar grupos de entrega.

> Por padrão, as sessões fazem roaming entre dispositivos cliente com o usuário. Quando o usuário inicia uma sessão e depois se move para outro dispositivo, a mesma sessão é usada e os aplicativos estão simultaneamente disponíveis em ambos os dispositivos. Você pode visualizar os aplicativos em vários dispositivos. Os aplicativos seguem, independentemente do dispositivo ou se existem sessões atuais. Frequentemente, impressoras e outros recursos atribuídos ao aplicativo também seguem.

Embora esse comportamento padrão ofereça muitas vantagens, ele pode não ser ideal em todos os casos. Você pode impedir o roaming de sessão usando o SDK do PowerShell.

Exemplo 1: Um profissional de saúde está usando dois dispositivos, preenchendo um formulário de seguro em um PC desktop e consultando informações do paciente em um tablet.

- Se o roaming de sessão estiver ativado, ambos os aplicativos aparecem em ambos os dispositivos (um aplicativo iniciado em um dispositivo é visível em todos os dispositivos em uso). Isso pode não atender aos requisitos de segurança.

- Se o roaming de sessão estiver desativado, o registro do paciente não aparece no PC desktop, e o formulário de seguro não aparece no tablet.

Exemplo 2: Um gerente de produção inicia um aplicativo no PC em seu escritório. O nome e a localização do dispositivo determinam quais impressoras e outros recursos estão disponíveis para essa sessão. Mais tarde no dia, ele vai para um escritório no prédio ao lado para uma reunião que exigirá o uso de uma impressora.

- Se o roaming de sessão estiver ativado, o gerente de produção provavelmente não conseguiria acessar as impressoras perto da sala de reunião, porque os aplicativos que ele iniciou anteriormente em seu escritório resultaram na atribuição de impressoras e outros recursos perto daquele local.
- Se o roaming de sessão estiver desativado, quando ele faz logon em uma máquina diferente (usando as mesmas credenciais), uma nova sessão é iniciada, e impressoras e recursos próximos ficam disponíveis.

Configurar roaming de sessão

Para configurar o roaming de sessão, use os seguintes cmdlets de regra de política de direito com a propriedade "SessionReconnection". Opcionalmente, você também pode especificar a propriedade "LeasingBehavior".

Para sessões de desktop:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

Para sessões de aplicativo:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

Onde `value` pode ser um dos seguintes:

- **Sempre:** As sessões sempre fazem roaming, independentemente do dispositivo cliente e se a sessão está conectada ou desconectada. Este é o valor padrão.
- **SomenteDesconectado:** Reconecte-se apenas a sessões que já estão desconectadas; caso contrário, inicie uma nova sessão. (As sessões podem fazer roaming entre dispositivos cliente desconectando-as primeiro ou usando o controle de espaço de trabalho para fazer o roaming explicitamente.) Uma sessão ativa conectada de outro dispositivo cliente nunca é usada. Em vez disso, uma nova sessão é iniciada.

- **SomenteMesmoPontoFinal:** Um usuário obtém uma sessão exclusiva para cada dispositivo cliente que ele usa. Isso desativa completamente o roaming. Os usuários podem se reconectar apenas ao mesmo dispositivo que foi usado anteriormente na sessão.

A propriedade "LeasingBehavior" é descrita abaixo.

Efeitos de outra configuração:

A desativação do roaming de sessão é afetada pelo limite de aplicativo "Permitir apenas uma instância do aplicativo por usuário" nas propriedades do aplicativo no Grupo de Entrega.

- Se você desativar o roaming de sessão, desative o limite de aplicativo "Permitir apenas uma instância...".
- Se você ativar o limite de aplicativo "Permitir apenas uma instância...", não configure nenhum dos dois valores que permitem novas sessões em novos dispositivos.

Intervalo de logon

Se uma máquina virtual contendo um VDA de desktop for encerrada antes que o processo de logon seja concluído, você poderá alocar mais tempo para o processo. O padrão para a versão 7.6 e posteriores é de 180 segundos (o padrão para 7.0-7.5 é de 90 segundos).

Na máquina (ou na imagem mestre usada em um catálogo de máquinas), defina a seguinte chave de registro:

Chave: `HKLM\SOFTWARE\Citrix\PortICA`

- Valor: `AutoLogonTimeout`
- Tipo: `DWORD`
- Especifique um tempo decimal em segundos, no intervalo de 0 a 3600.

Se você alterar a imagem mestre, implante a nova imagem no catálogo. Para obter mais informações, consulte Alterar a imagem mestre.

Essa configuração se aplica apenas a VMs com VDAs de desktop (estação de trabalho) de sessão única. A Microsoft controla o tempo limite de logon em máquinas com VDAs de servidor de várias sessões.

Tags

Introdução

Tags são strings que identificam itens como máquinas, aplicativos, desktops, grupos de entrega, grupos de aplicativos e políticas. Depois de criar uma tag e adicioná-la a um item, você pode adaptar certas operações para se aplicarem apenas a itens que possuem uma tag especificada.

- Personalizar exibições de pesquisa no Studio.

  Por exemplo, para exibir apenas aplicativos que foram otimizados para testadores, crie uma tag chamada “test” e adicione-a (aplique-a) a esses aplicativos. Agora você pode filtrar a pesquisa com a tag “test”.

- Publicar aplicativos de um grupo de aplicativos ou desktops específicos de um grupo de entrega, considerando apenas um subconjunto das máquinas nos grupos de entrega selecionados. Isso é chamado de *restrição de tag*.

  Com as restrições de tag, você pode usar suas máquinas existentes para mais de uma tarefa de publicação, economizando os custos associados à implantação e gerenciamento de mais máquinas. Uma restrição de tag pode ser pensada como a subdivisão (ou particionamento) das máquinas em um grupo de entrega. Sua funcionalidade é semelhante, mas não idêntica, aos grupos de trabalho em versões do XenApp anteriores à 7.x.

  Usar um grupo de aplicativos ou desktops com uma restrição de tag pode ser útil ao isolar e solucionar problemas de um subconjunto de máquinas em um grupo de entrega.

  Detalhes e exemplos do uso de uma restrição de tag são descritos posteriormente neste artigo.

- Agendar reinícios periódicos para um subconjunto de máquinas em um grupo de entrega.

  Usar uma restrição de tag para máquinas permite que você use novos cmdlets do PowerShell para configurar vários agendamentos de reinício para subconjuntos de máquinas em um grupo de entrega. Para exemplos e detalhes, consulte Gerenciar grupos de entrega.

- Adaptar a aplicação (atribuição) de políticas Citrix® a máquinas em grupos de entrega, tipos de grupo de entrega ou UOs que possuem (ou não possuem) uma tag especificada.

  Por exemplo, se você deseja aplicar uma política Citrix apenas às estações de trabalho mais potentes, adicione uma tag chamada “high power” a essas máquinas. Em seguida, na página **Atribuir Política** do assistente Criar Política, selecione essa tag e a caixa de seleção

Habilitar. Você também pode adicionar uma tag a um grupo de entrega e, em seguida, aplicar uma política Citrix a esse grupo. Para obter detalhes, consulte Criar políticas.

Você pode aplicar tags a:

- Máquinas
- Aplicativos
- Catálogos de máquinas
- Grupos de entrega
- Grupos de aplicativos

Você pode configurar uma restrição de tag ao criar ou editar o seguinte no Studio:

- Um desktop em um grupo de entrega compartilhado
- Um grupo de aplicativos

Importante:

Uma tag pode ser aplicada explicitamente a uma máquina ou pode ser aplicada explicitamente no nível do catálogo de máquinas ou do grupo de entrega. Quando uma tag é aplicada no nível do catálogo de máquinas ou do grupo de entrega, todas as máquinas dentro desse catálogo ou grupo de entrega herdam implicitamente a tag. Essas tags herdadas não podem ser removidas no nível da máquina. Para remover o efeito da tag, a tag deve ser removida do nível do catálogo de máquinas ou do grupo de entrega.

Restrições de tag para um desktop ou um grupo de aplicativos

Uma restrição de tag envolve várias etapas:

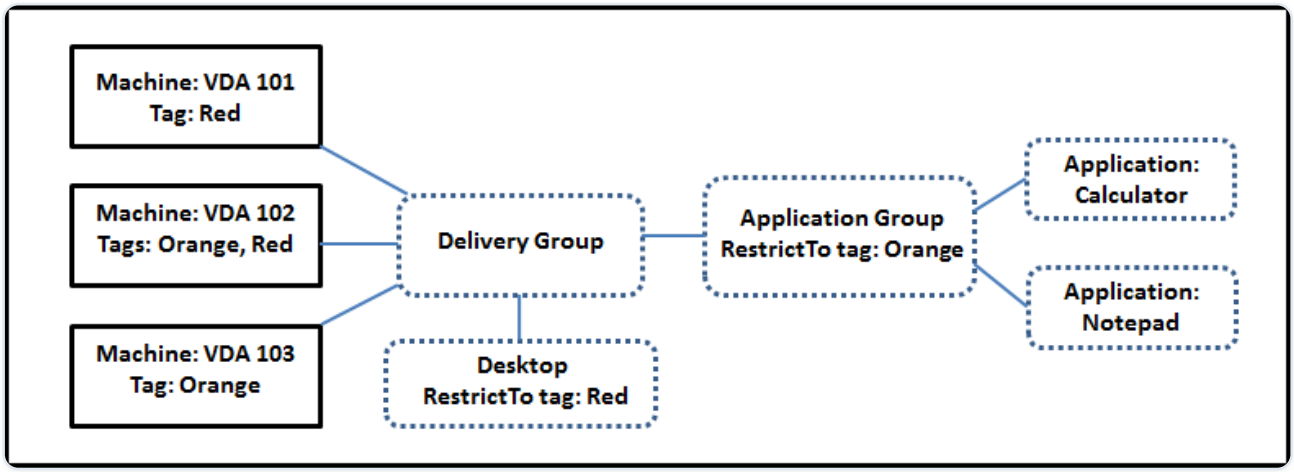
- Crie a tag e, em seguida, adicione (aplique) às máquinas.
- Crie ou edite um grupo com a restrição de tag (em outras palavras, restrinja os lançamentos a máquinas com a tag *x*).

Uma restrição de tag estende o processo de seleção de máquina do Controller. O Controller seleciona uma máquina de um grupo de entrega associado, sujeito à política de acesso, listas de usuários configuradas, preferência de zona e prontidão de lançamento, além da restrição de tag (se presente). Para aplicativos, o Controller recorre a outros grupos de entrega em ordem de

prioridade, aplicando as mesmas regras de seleção de máquina para cada grupo de entrega considerado.

Exemplo 1: Layout simples

Este exemplo apresenta um layout simples que usa restrições de tag para limitar quais máquinas são consideradas para determinados lançamentos de desktop e aplicativos. Há um grupo de entrega compartilhado, um desktop publicado e um grupo de aplicativos configurado com dois aplicativos.



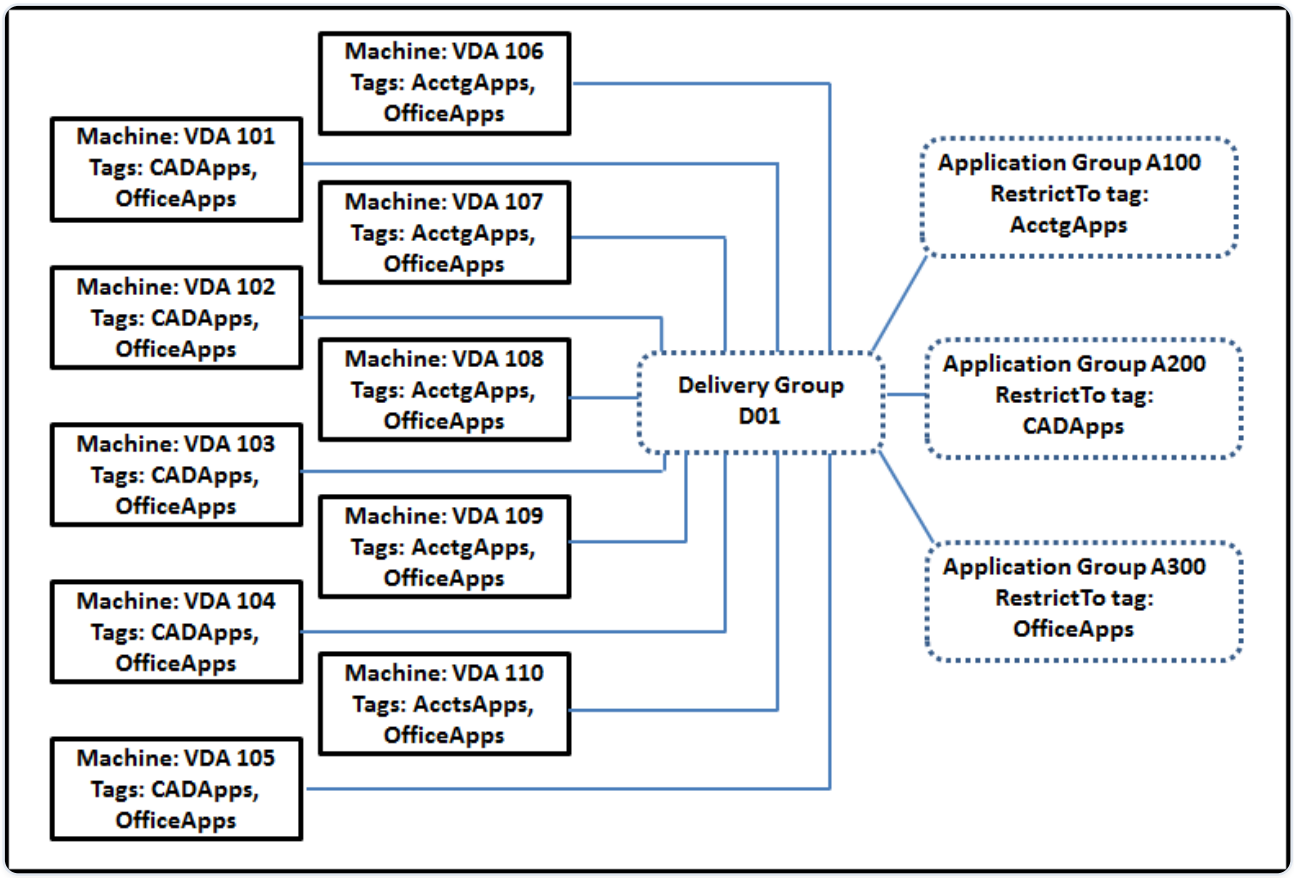
- Tags foram adicionadas a cada uma das três máquinas (VDA 101-103).
- O desktop no grupo de entrega foi criado com uma restrição de tag chamada `Red`. Assim, esse desktop pode ser iniciado apenas em máquinas nesse grupo de entrega que possuem a tag `Red`: VDA 101 e 102.
- O grupo de aplicativos foi criado com a restrição de tag `Orange`. Assim, cada um de seus aplicativos (`Calculator` e `Notepad`) pode ser iniciado apenas em máquinas nesse grupo de entrega que possuem a tag `Orange`: VDA 102 e 103.

A máquina VDA 102 possui ambas as tags (`Red` e `Orange`), então ela pode ser considerada para o lançamento dos aplicativos e do desktop.

Exemplo 2: Layout mais complexo

Este exemplo contém vários grupos de aplicativos que foram criados com restrições de tag. Isso resulta na capacidade de entregar mais aplicativos com menos máquinas do que seria necessário se você usasse apenas grupos de entrega.

Como configurar o exemplo 2 mostra as etapas usadas para criar e aplicar as tags e, em seguida, configurar as restrições de tag neste exemplo.



Este exemplo usa 10 máquinas (VDA 101-110), um grupo de entrega (`D01`) e três grupos de aplicativos (`A100` , `A200` , `A300`). Ao aplicar tags a cada máquina e, em seguida, especificar restrições de tag ao criar cada grupo de aplicativos:

- Usuários de contabilidade no grupo podem acessar os aplicativos de que precisam em cinco máquinas (VDA 101–105)
- Designers CAD no grupo podem acessar os aplicativos de que precisam em cinco máquinas (VDA 106-110)
- Usuários no grupo que precisam de aplicativos do Office podem acessar os aplicativos do Office em 10 máquinas (VDA 101-110)

Apenas 10 máquinas são usadas, com apenas um grupo de entrega. Usar apenas grupos de entrega (sem grupos de aplicativos) exigiria o dobro de máquinas, porque uma máquina pode pertencer a apenas um grupo de entrega.

Gerenciar tags e restrições de tags

As tags são criadas, adicionadas (aplicadas), editadas e excluídas de itens selecionados através da ação **Gerenciar Tags** no Studio.

(Exceção: As tags usadas para atribuições de política são criadas, editadas e excluídas através da ação **Gerenciar Tags**. No entanto, você aplica (atribui) tags ao criar a política. Consulte Criar políticas para obter detalhes.)

As restrições de tags são configuradas ao criar ou editar desktops em grupos de entrega e ao criar e editar grupos de aplicativos.

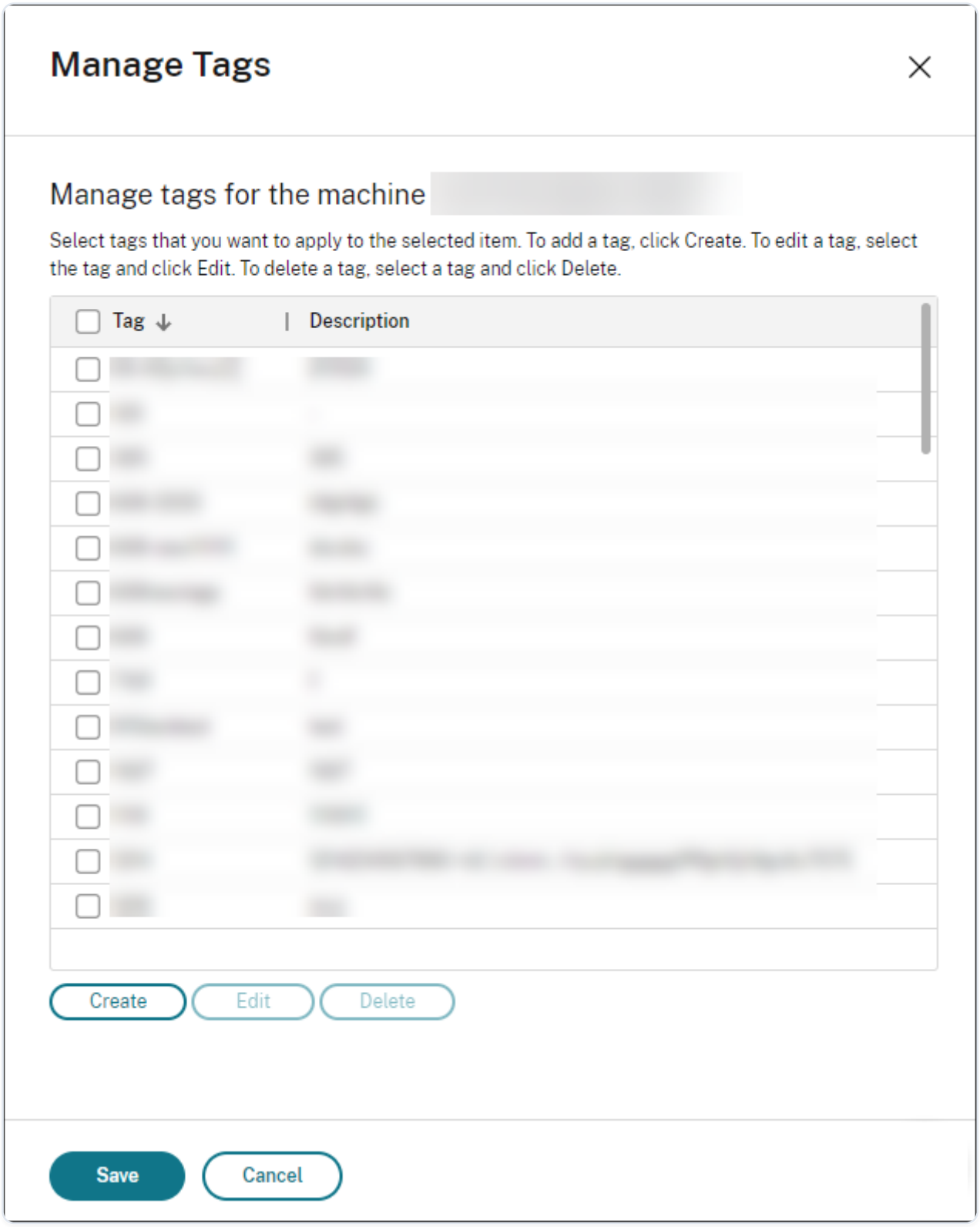
Usar o recurso Gerenciar Tags

No Studio, selecione os itens aos quais você deseja aplicar uma tag. Os itens incluem:

- Uma ou mais máquinas
- Um ou mais aplicativos
- Um desktop, um grupo de entrega ou um grupo de aplicativos
- Um catálogo de máquinas

Em seguida, selecione **Gerenciar Tags** na barra de ações. A caixa de diálogo **Gerenciar Tags** lista todas as tags existentes, não apenas as dos itens selecionados.

- Uma caixa de seleção ativada indica que a tag já foi adicionada aos itens selecionados. (Na captura de tela abaixo, a máquina selecionada tem uma tag chamada “Tag1” aplicada.)
- Se você selecionar mais de um item, uma caixa de seleção contendo um hífen indica que alguns, mas não todos os itens selecionados, têm essa tag adicionada.



As seguintes ações estão disponíveis na caixa de diálogo **Gerenciar Tags**. Consulte Precauções ao trabalhar com tags.

- **Para criar uma tag:**

  Selecione **Criar.** Insira um nome e uma descrição. Os nomes das tags devem ser exclusivos e não diferenciam maiúsculas de minúsculas. Em seguida, selecione **Salvar**.

A criação de uma tag não a aplica automaticamente a nenhum item selecionado. Use as caixas de seleção para aplicar a tag.

- **Para adicionar (aplicar) uma ou mais tags:**

  Marque a caixa de seleção ao lado do nome da tag. Uma caixa de seleção contendo um hífen indica que alguns, mas não todos os itens selecionados já têm a tag aplicada. Quando você seleciona vários itens e a caixa de seleção de uma tag tem um hífen, alterá-la para uma marca de seleção afeta todas as máquinas selecionadas.

  Se você tentar adicionar uma tag a máquinas, e essa tag for usada como restrição em um grupo de aplicativos, você será avisado de que a ação pode tornar essas máquinas disponíveis para inicialização. Se for essa a sua intenção, prossiga.

- **Para remover uma ou mais tags:**

  Desmarque a caixa de seleção ao lado do nome da tag. Uma caixa de seleção contendo um hífen indica que alguns, mas não todos os itens selecionados já têm a tag aplicada. Quando você seleciona vários itens e a caixa de seleção de uma tag tem um hífen, desmarcar a caixa de seleção remove a tag de todas as máquinas selecionadas.

  Se você tentar remover uma restrição de tag de uma máquina, você será avisado de que a ação pode afetar as máquinas consideradas para inicialização. Se for essa a sua intenção, prossiga.

- **Para editar uma tag:**

  Selecione uma tag e, em seguida, selecione **Editar**. Insira um novo nome, descrição ou ambos. Você pode editar apenas uma tag por vez.

- **Para excluir uma ou mais tags:**

  Selecione as tags e, em seguida, selecione **Excluir**. A caixa de diálogo **Excluir Tag** indica quantos itens usam atualmente as tags selecionadas (por exemplo, "2 máquinas"). Selecione um item para exibir mais informações (por exemplo, os nomes das duas máquinas que têm a tag aplicada). Confirme se deseja excluir as tags.

  Você não pode excluir uma tag que é usada como restrição. Primeiro, edite o grupo de aplicativos e remova a restrição de tag ou selecione uma tag diferente.

Quando terminar na caixa de diálogo **Gerenciar Tags**, selecione **Salvar**.

Para ver se uma máquina tem alguma tag aplicada: Selecione **Grupos de Entrega** no painel esquerdo. Selecione um grupo de entrega e, em seguida, selecione **Visualizar Máquinas** na

barra de ações. Selecione uma máquina e, em seguida, selecione a guia **Tags** no painel **Detalhes**.

Gerenciar restrições de tag

Configurar uma restrição de tag é um processo de várias etapas: Primeiro, você cria a tag e a adiciona/aplica às máquinas. Em seguida, você adiciona a restrição ao grupo de aplicativos ou à área de trabalho.

- **Criar e aplicar a tag:**

  Crie a tag e, em seguida, adicione (aplique)-a às máquinas que a restrição de tag afetará, usando as ações de **Gerenciar Tags**.

- **Para adicionar uma restrição de tag a um grupo de aplicativos:**

  Crie ou edite o grupo de aplicativos. Na página **Grupos de Entrega**, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag na lista.

- **Para alterar ou remover a restrição de tag em um grupo de aplicativos:**

  Edite o grupo. Na página **Grupos de Entrega**, selecione uma tag diferente da lista ou remova a restrição de tag completamente desmarcando **Restringir inicializações a máquinas com a tag**.

- **Para adicionar uma restrição de tag a uma área de trabalho:**

  Crie ou edite um grupo de entrega. Selecione **Adicionar** ou **Editar** na página **Áreas de Trabalho**. Na caixa de diálogo **Adicionar Área de Trabalho**, selecione **Restringir inicializações a máquinas com a tag** e, em seguida, selecione a tag no menu.

- **Para alterar ou remover a restrição de tag em um grupo de entrega:**

  Edite o grupo. Na página **Áreas de Trabalho**, selecione **Editar**. Na caixa de diálogo, selecione uma tag diferente da lista ou remova a restrição de tag completamente desmarcando **Restringir inicializações a máquinas com a tag**.

Precauções ao trabalhar com tags

Uma tag aplicada a um item pode ser usada para diferentes propósitos. Lembre-se de que adicionar, remover e excluir uma tag pode ter efeitos não intencionais. Você pode usar uma tag para classificar as exibições de máquinas ao usar a pesquisa no Studio. Você pode usar a mesma tag como uma restrição ao configurar um grupo de aplicativos ou uma área de trabalho. Essa ação

limita a consideração de inicialização apenas a máquinas em grupos de entrega especificados que possuem essa tag.

Se você adicionar uma tag a máquinas depois que essa tag for configurada como uma restrição de tag de grupo de desktop ou aplicativo, você será avisado de que isso pode tornar as máquinas disponíveis para iniciar mais aplicativos ou desktops. Se essa for sua intenção, prossiga. Caso contrário, cancele a operação.

Por exemplo, digamos que você crie um grupo de aplicativos com a restrição de tag `Red`. Mais tarde, você adiciona várias outras máquinas nos mesmos grupos de entrega usados por esse grupo de aplicativos. Se você tentar adicionar a tag `Red` a essas máquinas, verá uma mensagem semelhante a: "A tag `Red` é usada como restrição nos seguintes grupos de aplicativos. Adicionar esta tag pode tornar as máquinas selecionadas disponíveis para iniciar aplicativos neste grupo de aplicativos." Você pode então confirmar ou cancelar a adição dessa tag a essas máquinas adicionais.

Da mesma forma, quando uma tag é usada em um grupo de aplicativos para restringir inicializações, você não pode excluir a tag até editar o grupo e removê-la como uma restrição. (Se você pudesse excluir essa tag, isso poderia resultar em permitir que os aplicativos fossem iniciados em todas as máquinas nos grupos de entrega associados ao grupo de aplicativos.) A mesma proibição de exclusão de uma tag se aplica se a tag estiver sendo usada como uma restrição para inicializações de desktop. Depois de editar o grupo de aplicativos ou os desktops no grupo de entrega para remover essa restrição de tag, você pode excluir a tag.

Nem todas as máquinas podem ter os mesmos conjuntos de aplicativos. Um usuário pode pertencer a mais de um grupo de aplicativos, cada um com uma restrição de tag diferente e conjuntos de máquinas diferentes ou sobrepostos de grupos de entrega. A tabela a seguir lista como as considerações da máquina são decididas.

QUANDO UM APLICATIVO FOI ADICIONADO A	ESTAS MÁQUINAS NOS GRUPOS DE ENTREGA SELECIONADOS SÃO CONSIDERADAS PARA INICIALIZAÇÃO
Um grupo de aplicativos sem restrição de tag	Qualquer máquina.
Um grupo de aplicativos com restrição de tag A	Máquinas que têm a tag A aplicada.
Dois grupos de aplicativos, um com restrição de tag A e o outro com restrição de tag B	Máquinas que têm a tag A e a tag B. Se nenhuma estiver disponível, então máquinas que têm a tag A ou a tag B.

QUANDO UM APLICATIVO FOI ADICIONADO A	ESTAS MÁQUINAS NOS GRUPOS DE ENTREGA SELECIONADOS SÃO CONSIDERADAS PARA INICIALIZAÇÃO
Dois grupos de aplicativos, um com restrição de tag A e o outro sem restrição de tag	Máquinas que têm a tag A. Se nenhuma estiver disponível, então qualquer máquina.

Se você usou uma restrição de tag em um agendamento de reinicialização de máquina, quaisquer alterações que você fizer que afetem as aplicações ou restrições de tag afetarão o próximo ciclo de reinicialização da máquina. Isso não afeta nenhum ciclo de reinicialização que esteja em andamento enquanto as alterações estão sendo feitas.

Como configurar o exemplo 2

A sequência a seguir mostra as etapas para criar e aplicar tags e, em seguida, configurar restrições de tag para os grupos de aplicativos ilustrados no segundo exemplo anterior.

VDAs e aplicativos já foram instalados nas máquinas e o grupo de entrega foi criado.

Crie e aplique tags às máquinas:

1. No Studio, selecione **Delivery Groups** no painel esquerdo. Selecione o grupo de entrega `D01` e, em seguida, selecione **View Machines** na barra de ações.
2. Selecione as máquinas VDA 101-105 e, em seguida, selecione **Manage Tags** na barra de ações.
3. Na caixa de diálogo **Manage Tags**, selecione **Create**. Crie uma tag chamada `CADApps`. Selecione **OK**.
4. Selecione **Create** novamente e crie uma tag chamada `OfficeApps`. Selecione **OK**.
5. Adicione (aplique) as tags recém-criadas às máquinas selecionadas, marcando as caixas de seleção ao lado do nome de cada tag (`CADApps` e `OfficeApps`). Em seguida, feche a caixa de diálogo.
6. Selecione o grupo de entrega `D01`. Selecione **View Machines** na barra de ações.
7. Selecione as máquinas VDA 106-110 e, em seguida, selecione **Manage Tags** na barra de ações.
8. Na caixa de diálogo **Manage Tags**, selecione **Create**. Crie uma tag chamada `AcctgApps`. Selecione **OK**.

9. Aplique a tag `AcctgApps` recém-criada e a tag `OfficeApps` às máquinas selecionadas, marcando as caixas de seleção ao lado do nome de cada tag. Em seguida, feche a caixa de diálogo.

Crie os grupos de aplicativos com restrições de tag.

1. No Studio, selecione **Applications** no painel esquerdo.
2. Selecione **Criar Grupo de Aplicativos** na barra de ações. O assistente é iniciado.
3. Na página **Grupos de Entrega**, selecione o grupo de entrega `D01`. Selecione **Restringir inicializações a máquinas com tag** e então selecione a tag `AcctgApps` da lista.
4. Conclua o assistente, especificando os usuários de contabilidade e os aplicativos de contabilidade. (Ao adicionar o aplicativo, escolha a origem **Do menu Iniciar**, que procura o aplicativo nas máquinas que têm a tag `AcctgApps`.) Na página **Resumo**, nomeie o grupo `A100`.
5. Repita as etapas anteriores para criar o grupo de aplicativos `A200`, especificando máquinas que têm a tag `CADApps`, além dos usuários e aplicativos apropriados.
6. Repita as etapas para criar o grupo de aplicativos `A300`, especificando máquinas que têm a tag `OfficeApps`, além dos usuários e aplicativos apropriados.

Aplicar tags a catálogos de máquinas

Você pode usar o Studio ou o PowerShell para aplicar tags a catálogos de máquinas.

- O uso da interface de gerenciamento é descrito em Gerenciar tags. As exibições do catálogo não indicam se as tags são aplicadas.
- Para usar o PowerShell, consulte Usar o PowerShell para aplicar tags a catálogos.

Aqui está um exemplo de uso de tags com catálogos:

- Um grupo de entrega contém máquinas de vários catálogos, mas você deseja que uma operação (como um agendamento de reinicialização) afete apenas as máquinas em um catálogo específico. Aplicar uma tag a esse catálogo atinge esse objetivo.

Usar o PowerShell para aplicar tags a catálogos

Os seguintes cmdlets do PowerShell estão disponíveis:

- Você pode passar objetos de catálogo para cmdlets como `Add-BrokerTag` e `Remove-BrokerTag`.
- `Get-BrokerTagUsage` mostra quantos catálogos contêm tags.

- `Get-BrokerCatalog` tem uma propriedade chamada `Tags`.

Por exemplo, os seguintes cmdlets adicionam uma tag criada anteriormente chamada `fy2018` ao catálogo chamado `acctg`: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`.

Consulte a ajuda do cmdlet do PowerShell para obter orientação e sintaxe.

Tags automáticas

Usando tags automáticas, você pode definir regras para adição e remoção automáticas de tags em máquinas, grupos de aplicativos, aplicativos, grupos de desktops ou desktops. As tags também são removidas automaticamente se não atenderem às regras definidas. Esse aprimoramento elimina a necessidade de manter diferentes scripts que são executados periodicamente para otimização do ambiente.

Casos de uso

Com a marcação automática, você pode implementar regras relevantes para os seus impulsionadores de negócios, como redução de custos, otimização da infraestrutura e impulsionamento do consumo. A seguir, alguns dos casos de uso:

- **Recuperar VDIs não utilizados** - Para liberar as cargas de trabalho dedicadas que não foram usadas por mais de um número pré-configurado de dias para o pool disponível.
- **Remover desordem de aplicativos** - Para reduzir a desordem de aplicativos identificando os aplicativos que não foram usados por mais de um número pré-configurado de dias.
- **DGs com nível funcional inferior a X** - Para encontrar grupos de entrega com nível funcional inferior a um nível específico.
- **Usuários inativos** - Para recuperar recursos de usuários que não fizeram login por mais de um número pré-configurado de dias.

> **Nota:**
>
> A tag anexada a uma máquina que não foi usada por mais de 30 dias é removida dessa máquina na próxima vez que ela for executada, se um usuário fizer login nessa máquina após 30 dias.

Comandos PowerShell

Você pode criar autotags usando comandos PowerShell. Depois que uma regra de autotag é criada, ela é avaliada com uma frequência de 3600 segundos. Para obter mais informações, consulte New-BrokerAutoTagRule.

Os parâmetros de `New-BrokerAutoTagRule` são:

- Nome: Nome genérico para a regra
- Tipo de objeto: Máquina
- Texto da regra: O filtro para definir a regra.
- Uid da Tag: O ID da tag que você deseja associar.

Exemplos

1. Para marcar VDIs dedicados que não foram usados por mais de 30 dias:

   ```
   New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText
   “-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne
   `”InUse`” -and ( LastConnectionTime -lt ‘-30’ -or LastConnectionTime
   -eq `$null ) }” -TagUid 123
   ```

   Após a regra ser configurada, as máquinas com a tag **unused-VDI** são liberadas.

2. Para marcar grupos de entrega com nível funcional inferior a X (usando **L7_20** como o nível funcional limite):

   ```
   New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup'
   -RuleText " -Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid
   143
   ```

3. Para marcar aplicativos visíveis ao usuário publicados sem uma pasta:

   ```
   New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application'
   -RuleText "-Enabled $true -Filter { ClientFolder -eq $null } " -TagUid
   153`
   ```

Mais informações

Postagem do blog: Como atribuir desktops a servidores específicos.

Tarefas no Centro de Tarefas

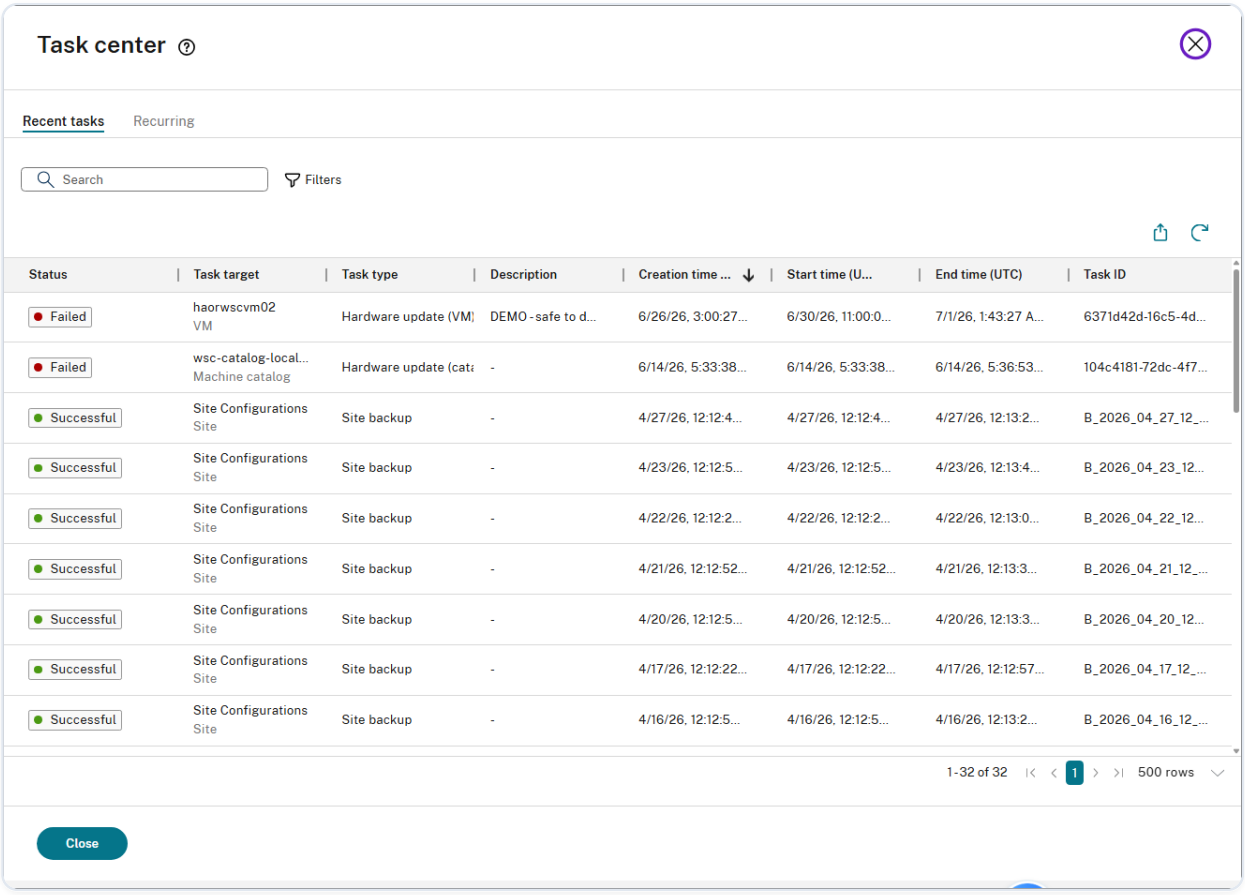
Centro de Tarefas oferece uma visão centralizada das tarefas agendadas e recorrentes no Citrix DaaS™. Você pode acompanhar o status das tarefas em tempo real e gerenciá-las a partir de um único local no Studio.

Acessar o Centro de Tarefas

1. Abra o console do Studio.
2. No canto superior direito, selecione o ícone **Calendário**.

   O painel do Centro de Tarefas é aberto.

   - A guia **Tarefas recentes** mostra execuções de tarefas individuais dos últimos 90 dias.
   - A guia **Recorrentes** mostra tarefas agendadas para serem executadas periodicamente ou no futuro.



Visualizar e gerenciar tarefas recentes

Na guia **Recentes**, você pode:

- Pesquisar e filtrar tarefas usando a barra de pesquisa.

- Acompanhar o status da tarefa em tempo real.
- Executar ações nas tarefas, como cancelar ou executar novamente.

Cada entrada de tarefa exibe os seguintes detalhes:

CAMPO	DESCRIÇÃO
Status	Estado atual da tarefa: Bem-sucedida, Cancelada, Em andamento ou Falha
Destino da Tarefa	Recurso ao qual a tarefa se aplica
Tipo de Tarefa	Tipo de operação (por exemplo, redefinição de disco do SO, backup de VM)
Descrição	Resumo da operação
ID da Tarefa	Identificador exclusivo para rastreamento

Visualizar e gerenciar tarefas recorrentes

Na guia **Recorrente**, você pode:

- Pesquisar e filtrar agendamentos recorrentes usando a barra de pesquisa.
- Acompanhe o estado de agendamentos recorrentes em tempo real.
- Execute ações em agendamentos recorrentes, como editar ou excluir.

Cada entrada recorrente exibe os seguintes detalhes:

CAMPO	DESCRIÇÃO
Estado	Estado atual do agendamento recorrente: Habilitado ou Desabilitado
Destino da Tarefa	Recurso ao qual o agendamento recorrente se aplica
Tipo de Tarefa	Tipo de operação, como backup do site ou agendamento de reinício
Nome do Agendamento	Nome do agendamento recorrente

CAMPO	DESCRIÇÃO
Descrição	Resumo da operação
Frequência	Frequência do agendamento recorrente: Diário, Semanal ou Mensal

Tipos de tarefa suportados

- Backup do site
- Agendamento de reinício

Solução de Problemas de Conexão do Citrix

O recurso Solução de Problemas de Conexão do Citrix foi projetado para capacitar os usuários finais a solucionar problemas potenciais de inicialização de desktops ou aplicativos de forma eficaz por conta própria. Este aprimoramento visa fornecer aos usuários diagnósticos claros, recomendações potenciais e a capacidade de executar correções com um simples clique.

Visão geral

O Citrix agora oferece mensagens de erro mais granulares e aprimoradas para ajudar os usuários a entender claramente a causa raiz das falhas de inicialização. O recurso Solução de Problemas de Conexão realiza uma análise em tempo real dos desafios de acessibilidade ao Virtual Delivery Agent (VDA) durante o processo de inicialização. Em seguida, ele apresenta mensagens de erro e recomendações amigáveis ao usuário, permitindo que os usuários resolvam o problema diretamente ou coletem logs para um tíquete de suporte, se necessário.

Caminhos de conexão analisados

O recurso diagnostica possíveis problemas de inicialização de aplicativos e desktops virtuais em pontos de conexão críticos, incluindo:

- Conectividade de rede do Cliente para o Gateway.
- Conexão do Gateway com o servidor StoreFront.
- Conexão do servidor StoreFront com o Broker.
- Conexão do Broker com o VDA.

Mensagens de erro e diagnósticos aprimorados

Em caso de falhas de inicialização, o Citrix agora exibe mensagens de erro claras e amigáveis ao usuário que identificam problemas de conexão específicos, como erros de rede, indisponibilidade do servidor ou falhas do VDA. Para administradores, códigos de erro detalhados são fornecidos nos logs, categorizados em erros do lado do servidor e do lado do cliente, servindo como referências valiosas para uma investigação mais aprofundada.

Autorrecuperação e ações de remediação

O recurso Solução de Problemas de Conexão do Citrix inclui etapas que os usuários podem seguir para se recuperar automaticamente de problemas comuns, minimizando assim a necessidade de intervenção do suporte. A seguir estão os problemas potenciais que podem ser resolvidos com remediação guiada:

- Reiniciar VDA
- Reiniciar o aplicativo Citrix Workspace (CWA) - Fazer login novamente no CWA
- Atualizar a lista de recursos
- Atualizar o aplicativo e tentar novamente
- Reconfigurar a loja
- Atualizar o CWA
- Reinstalar o CWA
- Verificar a rede
- Aguardar e tentar novamente

Requisitos do sistema

Para usar o recurso Solucionar Problemas de Conexão, tenha as seguintes versões do aplicativo Citrix Workspace:

- **Aplicativo Citrix Workspace para Mac:** Versão 2505 e posterior
- **Aplicativo Citrix Workspace para Windows:** Versão 2507 e posterior
- **Aplicativo Citrix Workspace para iOS:** Versão 2509 e posterior
- **Aplicativo Citrix Workspace para Android:** Versão 2509 e posterior

Como usar

O recurso Solucionar Problemas de Conexão é habilitado por padrão para ambientes Citrix DaaS. Mensagens de erro granulares e aprimoradas, juntamente com recomendações de correção, são fornecidas tanto para sessões iniciadas pelo navegador quanto para sessões iniciadas diretamente pelo aplicativo nativo Citrix Workspace.

Considerações importantes

Embora o recurso ofereça recursos robustos de autoatendimento, é importante observar o seguinte:

- A ação de correção "Reiniciar VDA" não oferece suporte a sessões iniciadas por meio de um modo de inicialização híbrido (ou seja, baixar um arquivo ICA de um navegador e, em seguida, iniciá-lo com o aplicativo nativo Citrix Workspace).

Códigos de erro

Os códigos de erro são divididos entre erros do lado do servidor e erros do lado do cliente. A seguir estão as tabelas com os códigos de erro.

Erros comuns do lado do servidor

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
`ResourceNotFound`	O recurso foi removido pelo seu administrador.	Para uma lista atualizada de aplicativos e desktops disponíveis, atualize o aplicativo Citrix Workspace ou faça logoff e login novamente.
`WorkstationInMaintenance`	O desktop está em manutenção planejada.	Aguarde até que a manutenção seja concluída e tente novamente.
`UnavailableDesktop`	Não há desktops disponíveis para conexão.	Aguarde alguns minutos e tente novamente. Se o problema persistir, entre em contato com o administrador do sistema.

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
`UnavailableAppProtectedDesktop`	Proteção de Aplicativo necessária para abrir recursos protegidos.	Atualize para uma versão do aplicativo Citrix Workspace com Proteção de Aplicativo ou entre em contato com o administrador do sistema para obter assistência.
`NotLicensed`	Não é possível iniciar o recurso porque o servidor não possui a licença apropriada.	Entre em contato com o administrador do sistema para obter assistência.
`NoMoreActiveSessions`	Não é possível iniciar o recurso porque não há slots de sessão disponíveis.	Aguarde alguns minutos e tente novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`GeneralAppLaunchError`	Ocorreu um erro desconhecido ao tentar abrir o recurso.	Entre em contato com o administrador do sistema para obter assistência.
`ResourceDisabled`	Seu administrador desabilitou o recurso.	Para obter uma lista atualizada de aplicativos e desktops disponíveis, atualize o aplicativo Citrix Workspace ou faça logoff e login novamente.

Aplicativo Citrix Workspace para Windows

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
`CertificateError`	Ocorreu um erro com o certificado do servidor.	Entre em contato com o administrador do sistema para obter assistência.
`PassthroughClientError`	Já existe uma sessão ativa.	Entre em contato com o administrador do sistema para obter assistência.

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
`IcaFileRetrieveError`	Ocorreu um erro ao tentar recuperar o arquivo ICA.	Entre em contato com o administrador do sistema para obter assistência.
`Icafileretrieveerrorreconnection`	Ocorreu um erro ao tentar recuperar o arquivo ICA durante a reconexão.	Entre em contato com o administrador do sistema para obter assistência.
`NoCWA`	O aplicativo Citrix Workspace é necessário para abrir recursos.	Instale o aplicativo Citrix Workspace ou entre em contato com o administrador do sistema para obter assistência.
`CouldNotFindStore`	Não foi possível recuperar a configuração de armazenamento necessária para iniciar o recurso.	Remova o armazenamento do aplicativo Citrix Workspace e adicione-o novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`noclientinstalled`	Não foi possível recuperar as informações necessárias para iniciar o recurso.	Atualize o aplicativo Citrix Workspace ou faça logoff e login novamente.
`AuthCancelled`	A sessão de autenticação expirou.	Para tentar resolver o problema, reautentique-se no aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`IcaFileLaunchError`	Ocorreu um erro ao tentar iniciar o arquivo ICA.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`CouldNotContactStore`	Ocorreu um erro ao tentar se comunicar com o VDA. Isso	Saia e reabra o aplicativo Citrix Workspace. Se o

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
	pode ser devido a um problema de conexão com o servidor.	problema persistir, entre em contato com o administrador do sistema.
`CCMError`	Não foi possível iniciar o recurso devido a um erro do Connection Manager. Código de erro: {errorCodeValue}	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`CCMInitFailed`	Não foi possível iniciar o recurso porque o Connection Manager falhou ao inicializar.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`CCMLoadFailed`	Não foi possível iniciar o recurso porque o Gerenciador de Conexão falhou ao carregar.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`InvalidIcaParams`	Não foi possível iniciar o recurso devido a parâmetros ICA incorretos.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`AppExiting`	Não foi possível iniciar o recurso porque o aplicativo Citrix Workspace está sendo encerrado.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`UTF8ConversionFailed`	Não foi possível analisar o arquivo ICA.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
`MissingSoftware`	Você precisa de software adicional para usar este aplicativo.	Entre em contato com o administrador do sistema para obter assistência.

Aplicativo Citrix Workspace para Mac

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
`AuthCancelled`	A sessão de autenticação expirou.	Para tentar resolver o problema, primeiro autenticar com suas credenciais. Se o problema persistir, entre em contato com o administrador do sistema.
`NetworkError`	Não foi possível iniciar o recurso devido a um problema de conexão de rede.	Verifique sua conexão e tente novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`ViewerNotFound`	O caminho do Citrix Viewer não pode ser encontrado.	Para tentar resolver o problema, desinstale e reinstale o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`ViewerOpenEventFailed`	O Citrix Viewer falhou ao criar um evento.	Tente iniciar o recurso de sua loja novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`ViewerLaunchTimeout`	O lançamento do Citrix Viewer expirou.	Tente iniciar o recurso da sua loja novamente. Se o problema persistir, entre em contato com o administrador do sistema.

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
`ViewerLaunchFailure`	O Citrix Viewer falhou ao iniciar.	Tente iniciar o recurso da sua loja novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`InvalidICAFile`	Não foi possível iniciar o recurso porque o arquivo ICA é inválido.	Tente iniciar o recurso da sua loja novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`CertificateError`	Ocorreu um erro com o certificado do servidor.	Entre em contato com o administrador do sistema para obter assistência.
`ResourceError`	Ocorreu um erro ao tentar iniciar o recurso. Isso pode ser devido a um problema de conexão com o servidor.	Aguarde alguns minutos e tente novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`UnknownError`	Ocorreu um erro desconhecido ao tentar abrir o recurso.	Aguarde alguns minutos e tente novamente. Se o problema persistir, entre em contato com o administrador do sistema.

Aplicativo Citrix Workspace para iOS

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
`credentialsMustChange`	Sua senha deve ser alterada.	Vá para as configurações da sua conta para alterar sua senha. Se o problema persistir, entre em contato com o administrador do sistema.

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
`noConfigurationFile`	Não foi possível recuperar os dados de configuração necessários.	Para tentar resolver o problema, remova a loja do aplicativo Citrix Workspace e adicione-a novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`http404Error`	Os recursos estão indisponíveis.	Entre em contato com o administrador do sistema para obter assistência.
`invalidTransactionId`	ID de transação inválido.	Aguarde alguns minutos e tente novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`credentialsExpired`	Sua senha expirou.	Vá para as configurações da sua conta para alterar sua senha. Se o problema persistir, entre em contato com o administrador do sistema.
`badAddressError`	Não foi possível encontrar o endereço do recurso.	Verifique sua conexão e tente novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`accountDisabled`	Sua conta está desativada.	Entre em contato com o administrador do sistema para obter assistência.
`accountLockedOut`	Sua conta está temporariamente bloqueada.	Entre em contato com o administrador do sistema para obter assistência.
`storeServerConnectionError`	Ocorreu um erro ao tentar se comunicar com o servidor.	Aguarde alguns minutos e tente novamente. Se o

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
		problema persistir, entre em contato com o administrador do sistema.
`internalServerError`	Ocorreu um erro desconhecido ao tentar se conectar ao servidor.	Entre em contato com o administrador do sistema para obter assistência.
`invalidXML`	Não foi possível abrir o recurso devido a um erro do serviço XML.	Entre em contato com o administrador do sistema para obter assistência.
`badCredentials`	Suas credenciais expiraram.	Para tentar resolver o problema, saia do aplicativo Citrix Workspace e faça login novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`appRemoved`	O recurso foi removido ou desativado pelo seu administrador.	Para uma lista atualizada de aplicativos e desktops disponíveis, atualize o aplicativo Citrix Workspace ou faça logoff e login novamente.
`invalidLogonHours`	Não é possível fazer login neste momento devido a restrições definidas pelo seu administrador.	Tente novamente durante o horário comercial normal. Se o problema persistir, entre em contato com o administrador do sistema.
`connectionError`	Não é possível conectar-se ao servidor. Isso pode ser devido a um problema de conexão de rede.	Para tentar resolver o problema, feche e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.

Aplicativo Citrix Workspace para Android

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
`http404Error`	Não é possível iniciar o recurso devido a um problema de conexão de rede.	Verifique sua conexão e tente novamente. Se o problema persistir, entre em contato com o administrador do sistema.
`couldNotConnectToWorkstation`	Não é possível conectar-se à área de trabalho.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`retryReasonRebooting`	Ocorreu um erro ao iniciar o recurso. A estação de trabalho solicitada está reiniciando.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`retryReasonResuming`	Ocorreu um erro ao iniciar o recurso. A estação de trabalho solicitada está sendo retomada.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`generalProblem`	Algo deu errado ao tentar abrir o recurso.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`retryReasonUnknown`	Ocorreu um erro no arquivo ICA.	Saia e reabra o aplicativo Citrix Workspace. Se o problema persistir, entre em contato com o administrador do sistema.
`appRemoved`	O recurso foi removido ou desabilitado pelo seu administrador.	Para uma lista atualizada de aplicativos e desktops disponíveis, atualize o aplicativo Citrix Workspace

ID DO ERRO	DESCRIÇÃO	RECOMENDAÇÃO
		ou faça logoff e login novamente.
`resourceError`	Ocorreu um erro ao tentar iniciar o arquivo ICA.	Aguarde alguns minutos e tente novamente. Se o problema persistir, entre em contato com o administrador do sistema. Reinicie o VDA se for uma máquina dedicada.
`resourceUnavailable`	Ocorreu um erro ao tentar iniciar o arquivo ICA.	Aguarde alguns minutos e tente novamente. Se o problema persistir, entre em contato com o administrador do sistema. Reinicie o VDA se for uma máquina dedicada.

Solucionar problemas de registro de VDA e inicialização de sessão

Oferecemos um recurso de verificação de integridade que permite avaliar a integridade dos VDAs. O recurso permite identificar possíveis causas para problemas comuns de registro de VDA e inicialização de sessão usando o Studio.

Ao contrário do Cloud Health Check, uma ferramenta autônoma para avaliar a integridade e a disponibilidade do site e de seus outros componentes, o recurso está disponível como a ação **Executar Verificação de Integridade** no Studio.

A ação **Executar Verificação de Integridade** pode executar as mesmas verificações que o Cloud Health Check, exceto as seguintes:

- Para registro de VDA:
  - Disponibilidade da porta de comunicação do VDA
- Para inicializações de sessão em VDAs:
  - Disponibilidade da porta de comunicação de inicialização da sessão

- Caminho de inicialização do aplicativo VDA

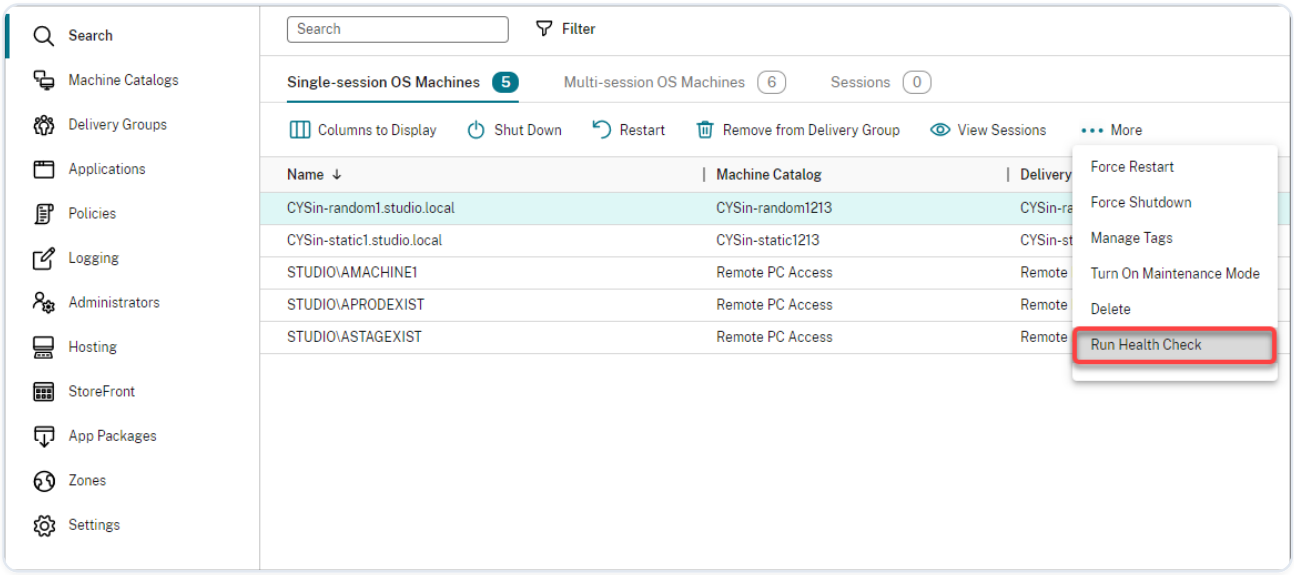
Pré-requisitos

Antes de usar o recurso, verifique se você atende aos seguintes pré-requisitos:

- VDAs do Windows
- VDA versão 2109 ou posterior
- VDAs registrados

Executar verificações de integridade para VDAs

1. No Studio, vá para o nó **Pesquisar**.
2. Selecione uma ou mais máquinas e, em seguida, selecione **Executar Verificação de Integridade** na barra de ações.



Nota:

Atualmente, você pode executar verificações de integridade apenas para VDAs registrados. A ação **Executar Verificação de Integridade** não está disponível para VDAs não registrados.

Depois de selecionar **Executar Verificação de Integridade**, uma janela é exibida, mostrando o progresso das verificações de integridade. Aguarde até que as verificações de

integridade sejam concluídas ou clique em **Cancelar** para cancelar as verificações. Se necessário, você pode mover a janela.



Nota:

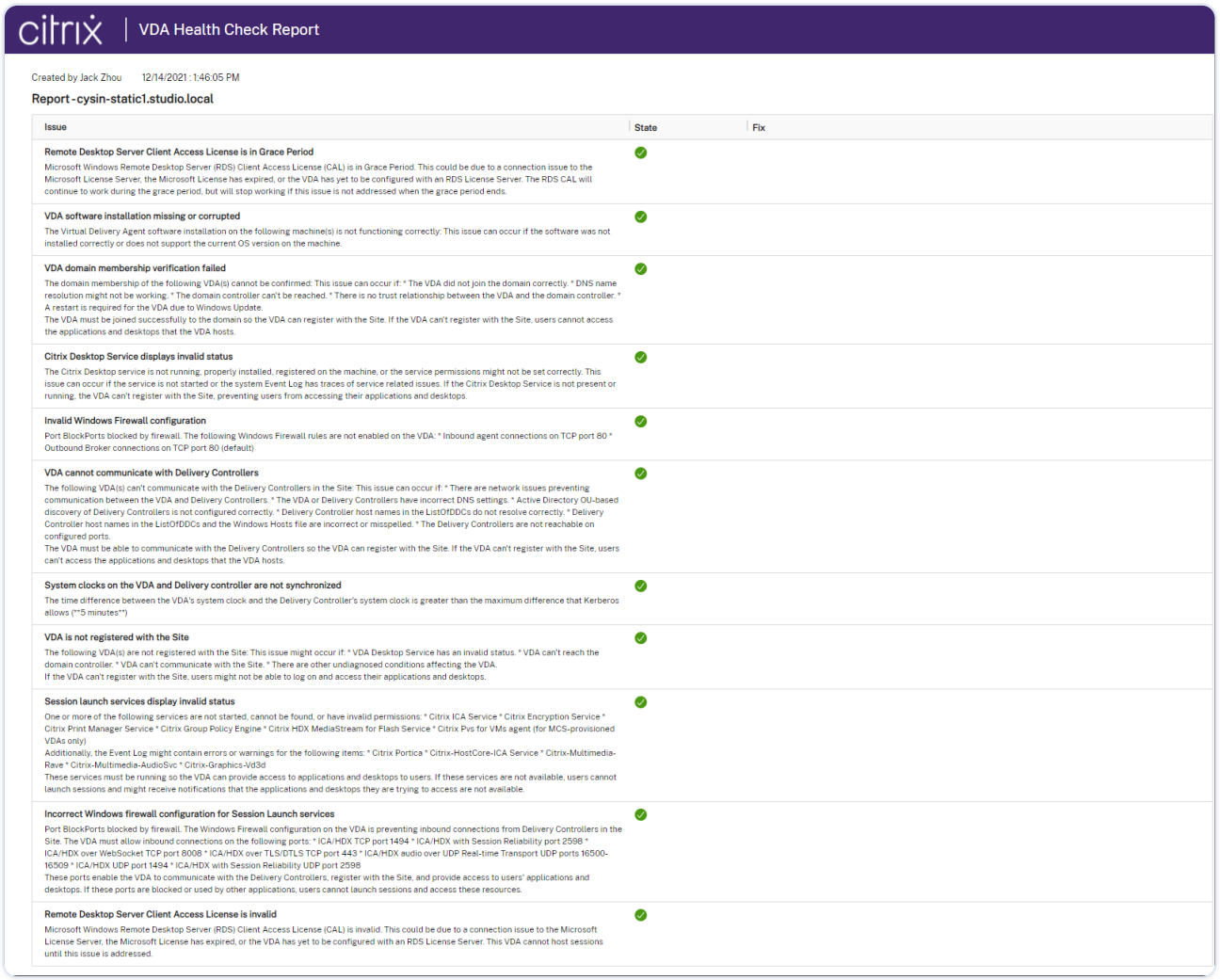
Em cenários onde uma janela de "verificações de integridade em andamento" já existe, você não pode executar verificações de integridade adicionais até que as verificações de integridade existentes sejam concluídas.

Após a conclusão das verificações de integridade, os dois botões a seguir aparecem: **Exibir relatório** e **Fechar**. Para visualizar os resultados das verificações de integridade, clique em **Exibir relatório**.



O relatório de verificação de integridade é aberto em uma nova guia do navegador. O relatório contém os seguintes elementos:

- Hora e data em que o relatório de resultados foi gerado
- A pessoa que executou as verificações de integridade
- Verificações executadas nas máquinas de destino
- Problemas encontrados, juntamente com recomendações de correção



citrix | VDA Health Check Report

Created by Jack Zhou 12/14/2021 : 1:46:05 PM

Report - cysin-static1.studio.local

Issue	State	Fix
Remote Desktop Server Client Access License is in Grace Period Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is in Grace Period. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. The RDS CAL will continue to work during the grace period, but will stop working if this issue is not addressed when the grace period ends.	✓	
VDA software installation missing or corrupted The Virtual Delivery Agent software installation on the following machine(s) is not functioning correctly: This issue can occur if the software was not installed correctly or does not support the current OS version on the machine.	✓	
VDA domain membership verification failed The domain membership of the following VDA(s) cannot be confirmed: This issue can occur if: * The VDA did not join the domain correctly. * DNS name resolution might not be working. * The domain controller can't be reached. * There is no trust relationship between the VDA and the domain controller. * A restart is required for the VDA due to Windows Update. The VDA must be joined successfully to the domain so the VDA can register with the Site. If the VDA can't register with the Site, users cannot access the applications and desktops that the VDA hosts.	✓	
Citrix Desktop Service displays invalid status The Citrix Desktop service is not running, properly installed, registered on the machine, or the service permissions might not be set correctly. This issue can occur if the service is not started or the system Event Log has traces of service related issues. If the Citrix Desktop Service is not present or running, the VDA can't register with the Site, preventing users from accessing their applications and desktops.	✓	
Invalid Windows Firewall configuration Port BlockPorts blocked by firewall. The following Windows Firewall rules are not enabled on the VDA: * Inbound agent connections on TCP port 80 * Outbound Broker connections on TCP port 80 (default)	✓	
VDA cannot communicate with Delivery Controllers The following VDA(s) can't communicate with the Delivery Controllers in the Site: This issue can occur if: * There are network issues preventing communication between the VDA and Delivery Controllers. * The VDA or Delivery Controllers have incorrect DNS settings. * Active Directory OU-based discovery of Delivery Controllers is not configured correctly. * Delivery Controller host names in the ListOfDDCs do not resolve correctly. * Delivery Controller host names in the ListOfDDCs and the Windows Hosts file are incorrect or misspelled. * The Delivery Controllers are not reachable on configured ports. The VDA must be able to communicate with the Delivery Controllers so the VDA can register with the Site. If the VDA can't register with the Site, users can't access the applications and desktops that the VDA hosts.	✓	
System clocks on the VDA and Delivery controller are not synchronized The time difference between the VDA's system clock and the Delivery Controller's system clock is greater than the maximum difference that Kerberos allows (**5 minutes**)	✓	
VDA is not registered with the Site The following VDA(s) are not registered with the Site: This issue might occur if: * VDA Desktop Service has an invalid status. * VDA can't reach the domain controller. * VDA can't communicate with the Site. * There are other undiagnosed conditions affecting the VDA. If the VDA can't register with the Site, users might not be able to log on and access their applications and desktops.	✓	
Session launch services display invalid status One or more of the following services are not started, cannot be found, or have invalid permissions: * Citrix ICA Service * Citrix Encryption Service * Citrix Print Manager Service * Citrix Group Policy Engine * Citrix HDX MediaStream for Flash Service * Citrix Pvs for VMs agent (for MCS-provisioned VDAs only) Additionally, the Event Log might contain errors or warnings for the following items: * Citrix Portica * Citrix-HostCore-ICA Service * Citrix-Multimedia-Rave * Citrix-Multimedia-AudioSvc * Citrix-Graphics-Vd3d These services must be running so the VDA can provide access to applications and desktops to users. If these services are not available, users cannot launch sessions and might receive notifications that the applications and desktops they are trying to access are not available.	✓	
Incorrect Windows firewall configuration for Session Launch services Port BlockPorts blocked by firewall. The Windows Firewall configuration on the VDA is preventing inbound connections from Delivery Controllers in the Site. The VDA must allow inbound connections on the following ports: * ICA/HDX TCP port 1494 * ICA/HDX with Session Reliability port 2598 * ICA/HDX over WebSocket TCP port 8008 * ICA/HDX over TLS/DTLS TCP port 443 * ICA/HDX audio over UDP Real-time Transport UDP ports 16500-16509 * ICA/HDX UDP port 1494 * ICA/HDX with Session Reliability UDP port 2598 These ports enable the VDA to communicate with the Delivery Controllers, register with the Site, and provide access to users' applications and desktops. If these ports are blocked or used by other applications, users cannot launch sessions and access these resources.	✓	
Remote Desktop Server Client Access License is invalid Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is invalid. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. This VDA cannot host sessions until this issue is addressed.	✓	

Você pode executar verificações de integridade individualmente e em lotes.

> **Nota:**
>
> Ao executar verificações de integridade em lotes, selecione no máximo 10 máquinas. Caso contrário, a ação **Executar Verificação de Integridade** estará indisponível.

Acesso do usuário

Existem dois componentes principais que fornecem acesso a aplicativos e desktops em implantações do Citrix DaaS™:

- **Citrix® StoreFront Cloud**: O Citrix® StoreFront Cloud é um serviço gerenciado pela Citrix. Esta é a maneira mais simples de fornecer acesso aos recursos do DaaS, não exigindo esforço de implantação e estando sempre atualizado com os recursos mais recentes.

- **Citrix StoreFront**: O Citrix StoreFront é um produto local que você instala em seu próprio ambiente. Isso é recomendado quando você precisa agregar recursos de implantações DaaS e CVAD locais ou quando precisa de mais controle da implantação. Você pode implantar um Citrix Gateway para permitir que os usuários autenticar e se conectem ao StoreFront de fora da sua rede interna.

Em ambos os casos, os usuários finais acessam seus espaços de trabalho ou lojas usando o aplicativo Citrix Workspace, seja em um navegador da web ou em um aplicativo instalado localmente.

Usando o Citrix® StoreFront Cloud

O acesso às lojas ocorre por meio de uma ou mais URLs `https://<subdomain>.cloud.com`, onde você pode escolher `<subdomain>`. Alternativamente, você pode registrar seu próprio domínio personalizado.

Para obter mais informações sobre como usar o Citrix® StoreFront Cloud, consulte:

- Configurar acesso: Para configurar o acesso.
- Configurar autenticação: Para configurar a autenticação.
- Gerenciar sua experiência de espaço de trabalho: Para entender como os usuários finais acessam seu espaço de trabalho e como ele aparece.

Para fornecer acesso remoto aos recursos gerenciados pelo DaaS, você pode usar o serviço Citrix Gateway ou seu próprio Citrix Gateway. Para obter mais informações sobre como configurar o acesso remoto aos recursos, consulte Conectividade com recursos DaaS.

Continuidade do serviço

A continuidade do serviço permite que os usuários conectem recursos quando o Citrix Cloud não está disponível. Para obter mais informações, consulte Continuidade do serviço.

Usando o StoreFront local

StoreFront é um aplicativo Windows que você pode instalar em seus próprios servidores para fornecer acesso a recursos CVAD, DaaS e SPA. Ele se conecta ao DaaS usando Citrix Cloud Connectors que atua como proxy para as solicitações para o Citrix Cloud. O conector criptografa as senhas antes que sejam enviadas para o Citrix Cloud, usando uma chave que é retornada diretamente para o aplicativo Citrix Workspace e nunca enviada para a nuvem.

1. Instale os conectores e habilite HTTPS. Você deve ter pelo menos dois conectores em cada local para redundância.
2. Certifique-se de que o Cloud Connector possa alcançar a URL do Cloud NFuse/STA em (`https://<customername\>.xendesktop.net/Scripts/wpnbr.dll` e `ctxsta.dll`).
3. Se você ainda não tiver uma implantação do StoreFront, instale o StoreFront e crie uma implantação.
4. Adicione um site à sua loja. Na lista de servidores, inclua todos os conectores de nuvem de todos os locais de recursos. Escolha o protocolo HTTPS.

Acesso do usuário final

Para fornecer acesso aos usuários finais usando o aplicativo Citrix Workspace, consulte Opções de acesso do usuário

Acesso remoto usando o Citrix Gateway

Você não deve expor seu servidor StoreFront diretamente à internet. Em vez disso, forneça autenticação e acesso remoto usando o Citrix Gateway. Você também pode usar um Citrix Gateway para acesso interno para aproveitar seus recursos de segurança.

- Implante um dispositivo NetScaler Gateway. Consulte a documentação do NetScaler Gateway para obter detalhes.
- Configure o Gateway para acesso remoto à sua loja. Para os servidores STA, você pode usar os Cloud Connectors.
- Adicione o Citrix Gateway ao StoreFront. Use a mesma lista de servidores STA que você configurou em seu gateway.

Cache de Host Local

O Cache de Host Local permite que as operações de corretagem de conexão na implantação do Citrix DaaS continuem quando os Cloud Connectors não conseguem se comunicar com o Citrix Cloud.

O recurso Cache de Host Local requer um Citrix® StoreFront local implantado pelo cliente.

Cada local de recurso deve ter um StoreFront local implantado pelo cliente. Verifique se o local de recurso contém um StoreFront local que aponta para todos os Cloud Connectors nesse local de recurso.

Para obter mais informações, consulte Cache de Host Local.

IP virtual e loopback virtual

> **Importante:**
>
> O Windows 10 Enterprise multi-session não oferece suporte à Virtualização de IP de Área de Trabalho Remota (IP Virtual) e não oferecemos suporte a IP Virtual nem a loopback virtual no Windows 10 Enterprise multi-session.

> Os recursos de IP virtual e loopback virtual são suportados em máquinas Windows Server 2016. Esses recursos não se aplicam a máquinas com sistema operacional Windows desktop.

O recurso de endereço IP virtual da Microsoft fornece a um aplicativo publicado um endereço IP exclusivo atribuído dinamicamente para cada sessão. O recurso de loopback virtual da Citrix permite configurar aplicativos que dependem de comunicações com localhost (127.0.0.1 por padrão) para usar um endereço de loopback virtual exclusivo no intervalo de localhost (127.*).

Certos aplicativos, como CRM e Computer Telephony Integration (CTI), usam um endereço IP para endereçamento, licenciamento, identificação ou outros propósitos e, portanto, exigem um endereço IP exclusivo ou um endereço de loopback nas sessões. Outros aplicativos podem se vincular a uma porta estática, então as tentativas de iniciar instâncias adicionais de um aplicativo em um ambiente multiusuário falharão porque a porta já está em uso. Para que tais aplicativos funcionem corretamente em um ambiente Citrix Virtual Apps™, é necessário um endereço IP exclusivo para cada dispositivo.

IP virtual e loopback virtual são recursos independentes. Você pode usar um ou ambos.

Sinopse da ação do administrador:

- Para usar o IP virtual da Microsoft, habilite-o e configure-o no servidor Windows. (As configurações de política do Citrix® não são necessárias.)
- Para usar o loopback virtual da Citrix, configure duas configurações em uma política da Citrix.

IP virtual

Quando o IP virtual é habilitado e configurado no servidor Windows, cada aplicativo configurado em execução em uma sessão parece ter um endereço exclusivo. Os usuários acessam esses

aplicativos em um servidor Citrix Virtual Apps da mesma forma que acessam qualquer outro aplicativo publicado. Um processo requer IP virtual em qualquer um dos seguintes casos:

- O processo usa um número de porta TCP codificado
- O processo usa soquetes do Windows e requer um endereço IP exclusivo ou um número de porta TCP especificado

Para determinar se um aplicativo precisa usar endereços IP virtuais:

1. Obtenha a ferramenta TCPView da Microsoft. Esta ferramenta lista todos os aplicativos que vinculam endereços IP e portas específicos.
2. Desative o recurso Resolver Endereços IP para que você veja os endereços em vez dos nomes de host.
3. Inicie o aplicativo e use o TCPView para ver quais endereços IP e portas são abertos pelo aplicativo e quais nomes de processo estão abrindo essas portas.
4. Configure quaisquer processos que abram o endereço IP do servidor, 0.0.0.0 ou 127.0.0.1.
5. Para garantir que um aplicativo não abra o mesmo endereço IP em uma porta diferente, inicie uma instância adicional do aplicativo.

Como funciona a virtualização de IP do Microsoft Remote Desktop (RD)

- O endereçamento IP virtual deve ser habilitado no servidor Microsoft.

  Por exemplo, em um ambiente Windows Server 2016, no Gerenciador do Servidor, expanda **Serviços de Área de Trabalho Remota > Conexões do Host da Sessão RD** para habilitar o recurso de Virtualização de IP RD e configurar as definições para atribuir dinamicamente endereços IP usando o servidor Dynamic Host Configuration Protocol (DHCP) por sessão ou por programa. Consulte a documentação da Microsoft para obter instruções.
- Após o recurso ser habilitado, na inicialização da sessão, o servidor solicita endereços IP atribuídos dinamicamente do servidor DHCP.
- O recurso de Virtualização de IP RD atribui endereços IP a conexões de área de trabalho remota por sessão ou por programa. Se você atribuir endereços IP para vários programas, eles compartilharão um endereço IP por sessão.
- Depois que um endereço é atribuído a uma sessão, a sessão usa o endereço virtual em vez do endereço IP principal do sistema sempre que as seguintes chamadas são feitas: `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Ao usar o recurso de virtualização de IP da Microsoft na configuração de hospedagem de sessão da Área de Trabalho Remota, os aplicativos são vinculados a endereços IP específicos inserindo um componente de “filtro” entre o aplicativo e as chamadas de função Winsock. O aplicativo então vê apenas o endereço IP que deve usar. Qualquer tentativa do aplicativo de escutar comunicações TCP ou UDP é vinculada automaticamente ao seu endereço IP virtual alocado (ou endereço de loopback), e quaisquer conexões de origem abertas pelo aplicativo se originam do endereço IP vinculado ao aplicativo.

Em funções que retornam um endereço (como `GetAddrInfo()`, que é controlado por uma política do Windows), se o endereço IP do host local for solicitado, o IP virtual examina o endereço IP retornado e o altera para o endereço IP virtual da sessão. Aplicativos que tentam obter o endereço IP do servidor local por meio de tais funções de nome veem apenas o endereço IP virtual exclusivo atribuído a essa sessão. Este endereço IP é frequentemente usado em chamadas de soquete subsequentes, como bind ou connect. Para obter mais informações sobre políticas do Windows, consulte Virtualização de IP RDS no Windows Server.

Frequentemente, um aplicativo solicita vincular-se a uma porta para escutar no endereço 0.0.0.0. Quando um aplicativo faz isso e usa uma porta estática, você não pode iniciar mais de uma instância do aplicativo. O recurso de endereço IP virtual também procura por 0.0.0.0 nesses tipos de chamada e altera a chamada para escutar no endereço IP virtual específico, o que permite que mais de um aplicativo escute na mesma porta no mesmo computador porque todos estão escutando em endereços diferentes. A chamada é alterada apenas se estiver em uma sessão ICA e o recurso de endereço IP virtual estiver habilitado. Por exemplo, se duas instâncias de um aplicativo em execução em sessões diferentes tentarem vincular-se a todas as interfaces (0.0.0.0) e a uma porta específica (como 9000), elas serão vinculadas a VIPAddress1:9000 e VIPAddress2:9000 e não haverá conflito.

Loopback virtual

Habilitar as configurações da política de loopback de IP virtual da Citrix permite que cada sessão tenha seu próprio endereço de loopback para comunicação. Quando um aplicativo usa o endereço localhost (padrão = 127.0.0.1) em uma chamada Winsock, o recurso de loopback virtual simplesmente substitui 127.0.0.1 por 127.X.X.X, onde X.X.X é uma representação do ID da sessão + 1. Por exemplo, um ID de sessão de 7 é 127.0.0.8. No caso improvável de o ID da sessão exceder o quarto octeto (mais de 255), o endereço passa para o próximo octeto (127.0.1.0), até o máximo de 127.255.255.255.

Um processo requer loopback virtual em qualquer um dos seguintes casos:

- O processo usa o endereço de loopback (localhost) do soquete do Windows (127.0.0.1)

- O processo usa um número de porta TCP codificado

Use as configurações da política de loopback virtual para aplicativos que usam um endereço de loopback para comunicação entre processos. Nenhuma configuração adicional é necessária. O loopback virtual não tem dependência de IP Virtual, então você não precisa configurar o servidor Microsoft.

- Suporte a loopback de IP virtual. Quando ativada, esta configuração de política permite que cada sessão tenha seu próprio endereço de loopback virtual. Esta configuração está desativada por padrão. O recurso se aplica apenas a aplicativos especificados com a configuração de política da lista de programas de loopback virtual de IP virtual.
- Lista de programas de loopback virtual de IP virtual. Esta configuração de política especifica os aplicativos que usam o recurso de loopback de IP virtual. Esta configuração se aplica apenas quando a configuração de política de suporte a loopback de IP virtual está ativada.

Recurso relacionado

Você pode usar as seguintes configurações de registro para garantir que o loopback virtual tenha preferência sobre o IP virtual; isso é chamado de loopback preferencial. No entanto, prossiga com cautela:

- Use o loopback preferencial apenas se o IP Virtual e o loopback virtual estiverem ativados; caso contrário, você poderá ter resultados inesperados.
- A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Execute regedit nos servidores onde os aplicativos residem.

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- Nome: PreferLoopback, Tipo: REG_DWORD, Dados: 1
- Nome: PreferLoopbackProcesses, Tipo: REG_MULTI_SZ, Dados: \<lista de processos\>

Zonas

Introdução

As implantações do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™) que abrangem locais amplamente dispersos conectados por uma WAN podem enfrentar desafios de latência e confiabilidade da rede. O uso de zonas pode ajudar os usuários em regiões remotas a se conectar a recursos sem necessariamente forçar suas conexões a atravessar grandes segmentos da WAN. Em um ambiente Citrix DaaS, cada local de recurso é considerado uma zona.

As zonas podem ser úteis em implantações de todos os tamanhos. Você pode usar zonas para manter aplicativos e desktops mais próximos dos usuários, o que melhora o desempenho. As zonas podem ser usadas para recuperação de desastres, data centers geograficamente distantes, filiais, uma nuvem ou uma zona de disponibilidade em uma nuvem.

Ao longo deste artigo, o termo local refere-se à zona em discussão. Por exemplo, "Um VDA se registra em um Cloud Connector local" significa que um VDA se registra em um Cloud Connector na zona onde o VDA está localizado.

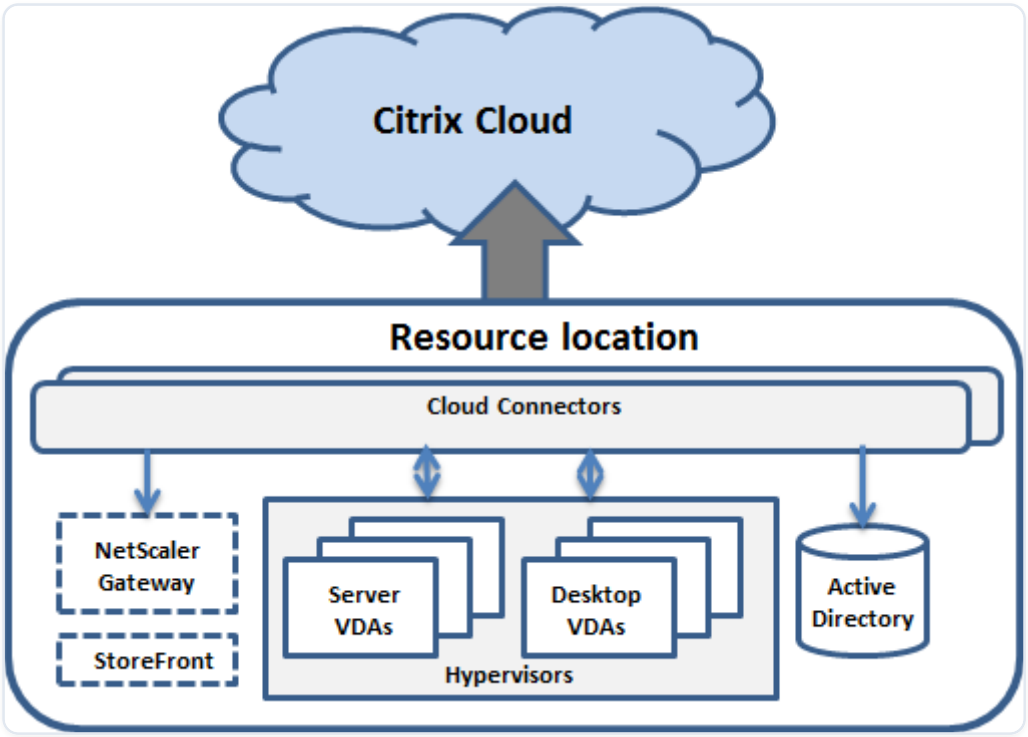
Diferenças das zonas em ambientes Citrix Virtual Apps and Desktops locais

As zonas no ambiente Citrix DaaS™ são semelhantes, mas não idênticas às zonas em uma implantação local do Citrix Virtual Apps and Desktops.

- No Citrix DaaS, as zonas são criadas automaticamente quando você cria um local de recurso e adiciona um Cloud Connector a ele. Ao contrário de uma implantação local, o ambiente Citrix DaaS não classifica as zonas como primárias ou satélites.
- No XenApp versão 6.5 e anteriores, as zonas incluíam coletores de dados. O Citrix DaaS não usa coletores de dados para zonas. Além disso, o failover e as zonas preferenciais funcionam de forma diferente.

O que há em uma zona

Uma zona é equivalente a um local de recurso. Ao criar um local de recurso e instalar um Cloud Connector, uma zona é criada automaticamente para você. Cada zona pode ter um conjunto diferente de recursos, com base nas suas necessidades e ambiente exclusivos.



Cada zona deve sempre ter pelo menos um Cloud Connector e, preferencialmente, dois ou mais, para redundância.

Você pode colocar catálogos de máquinas, hypervisors, conexões de host, usuários e aplicativos em uma zona. Uma zona também pode conter um Citrix Gateway.

A colocação de itens em uma zona afeta como o Citrix DaaS interage com eles e com outros objetos relacionados a eles.

- Quando uma conexão de hipervisor é colocada em uma zona, presume-se que todos os hipervisores gerenciados por meio dessa conexão também residam nessa zona.
- Quando um catálogo de máquinas é colocado em uma zona, presume-se que todos os VDAs no catálogo estejam na zona.
- Instâncias do Citrix Gateway podem ser adicionadas a zonas. Ao criar um local de recurso, é oferecida a opção de adicionar um Citrix Gateway. Quando um Citrix Gateway é associado a uma zona, ele é preferencialmente usado quando as conexões com VDAs nessa zona são utilizadas.
- Idealmente, o Citrix Gateway em uma zona é usado para conexões de usuário que chegam a essa zona de outras zonas ou locais externos. Você também pode usá-lo para conexões dentro da zona.
- Depois de criar mais locais de recursos e instalar Cloud Connectors neles (o que cria automaticamente mais zonas), você pode mover recursos entre as zonas. Essa flexibilidade vem com o risco de separar itens que funcionam melhor em proximidade. Por exemplo, mover

um catálogo para uma zona diferente da conexão (host) que cria as máquinas no catálogo pode afetar o desempenho. Portanto, considere os possíveis efeitos não intencionais antes de mover itens entre zonas. Mantenha um catálogo e a conexão de host que ele usa na mesma zona.

Se a conexão entre uma zona e o Citrix Cloud falhar, o recurso Local Host Cache permite que um Cloud Connector na zona continue intermediando conexões com VDAs nessa zona. (A zona deve ter o StoreFront instalado.) Por exemplo, isso é eficaz em um escritório onde os trabalhadores usam o site local do StoreFront para acessar seus recursos locais, mesmo que o link WAN que conecta o escritório à rede corporativa falhe. Para obter mais informações, consulte Cache de Host Local.

Onde os VDAs se registram

Os VDAs devem ter a versão mínima 7.7 para usar estes recursos de registro de zona:

- Um VDA em uma zona se registra com um Cloud Connector local.
  - Enquanto esse Cloud Connector puder se comunicar com o Citrix Cloud™, as operações normais continuarão.
  - Se esse Cloud Connector estiver operacional, mas não puder se comunicar com o Citrix Cloud (e essa zona tiver um StoreFront local), ele entrará no modo de interrupção do Local Host Cache.
  - Se um Cloud Connector falhar, os VDAs nessa zona tentarão se registrar com outros Cloud Connectors locais. Um VDA em uma zona nunca tenta se registrar com um Cloud Connector em outra zona.
- Se você adicionar ou remover um Cloud Connector em uma zona (usando o console de gerenciamento do Citrix Cloud) e a atualização automática estiver habilitada, os VDAs nessa zona receberão listas atualizadas de Cloud Connectors locais disponíveis, para que saibam com quem podem se registrar e de quem podem aceitar conexões.
- Se você mover um catálogo de máquinas para outra zona (usando o Studio), os VDAs nesse catálogo se registrarão novamente com os Cloud Connectors na zona para onde você moveu o catálogo. Ao mover um catálogo, certifique-se de também mover qualquer conexão de host associada para a mesma zona.
- Durante uma interrupção (quando os Cloud Connectors em uma zona não conseguem se comunicar com o Citrix Cloud), apenas os recursos associados às máquinas registradas nessa zona estarão disponíveis.

Preferência de zona

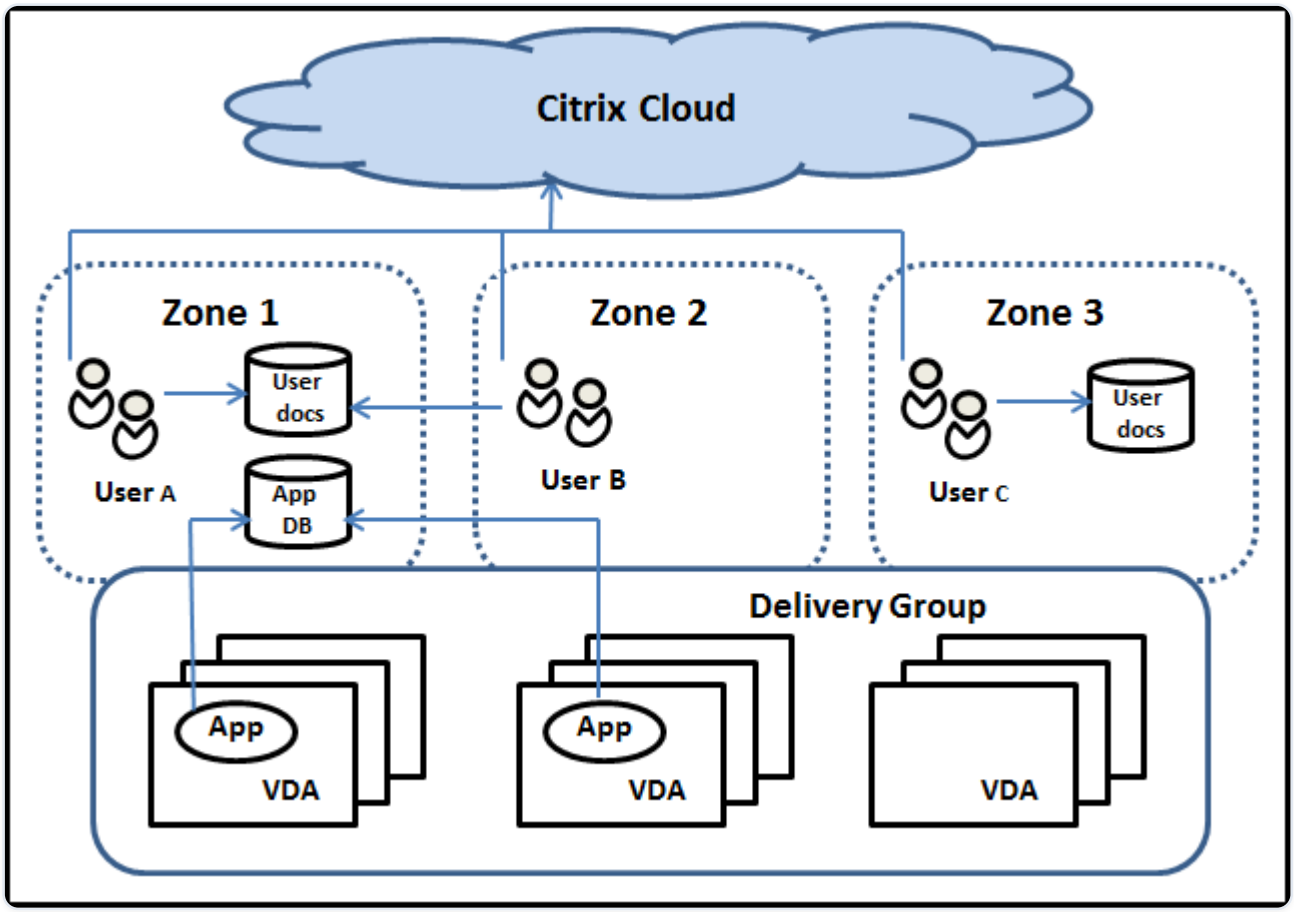
Em um Site com várias zonas, o recurso de preferência de zona oferece ao administrador mais flexibilidade para controlar qual VDA é usado para iniciar um aplicativo ou desktop.

Como funciona a preferência de zona

Existem três formas de preferência de zona. Você pode preferir usar um VDA em uma zona específica, com base em:

- Onde os dados do aplicativo são armazenados. Isso é chamado de home do aplicativo.
- O local dos dados home do usuário, como um perfil ou compartilhamento home. Isso é chamado de home do usuário.
- A localização atual do usuário (onde o aplicativo Citrix Workspace está sendo executado). Isso é chamado de localização do usuário. A localização do usuário requer no mínimo StoreFront 3.7 e Citrix Gateway (anteriormente NetScaler Gateway) 11.0-65.x.

O gráfico a seguir mostra um exemplo de configuração multizona.



Neste exemplo, os VDAs estão distribuídos entre três zonas, mas todos estão no mesmo grupo de entrega. Portanto, o broker do Citrix DaaS pode ter uma escolha de qual VDA usar para uma solicitação de inicialização do usuário. Este exemplo ilustra que os usuários podem estar

executando seus endpoints do aplicativo Citrix Workspace em diferentes locais. O Usuário A está usando um dispositivo com o aplicativo Citrix Workspace na zona 1. O Usuário B está usando um dispositivo na zona 2. Da mesma forma, os documentos de um usuário podem ser armazenados em diferentes locais. Os Usuários A e B usam um compartilhamento localizado na zona 1. O Usuário C usa um compartilhamento na zona 3. Além disso, um dos aplicativos publicados usa um banco de dados localizado na zona 1.

Você associa um usuário ou aplicativo a uma zona configurando uma zona home para o usuário ou aplicativo. O broker então usa essas associações para ajudar a selecionar a zona onde uma sessão será iniciada, se houver recursos disponíveis. Você:

- Configure a zona home para um usuário adicionando um usuário a uma zona.
- Configure a zona home para um aplicativo editando as propriedades do aplicativo.

Um usuário ou um aplicativo pode ter apenas uma zona home por vez. (Uma exceção para usuários pode ocorrer quando várias associações de zona acontecem devido à associação a grupos de usuários. No entanto, mesmo neste caso, o broker usa apenas uma zona home.)

Embora as preferências de zona para usuários e aplicativos possam ser configuradas, o broker seleciona apenas uma zona preferencial para um lançamento. A ordem de prioridade padrão para selecionar a zona preferencial é: home do aplicativo > home do usuário > localização do usuário. Quando um usuário inicia um aplicativo:

- Se essa aplicação tiver uma associação de zona configurada (uma zona inicial da aplicação), então a zona preferencial é a zona inicial para essa aplicação.
- Se a aplicação não tiver uma associação de zona configurada, mas o usuário tiver (uma zona inicial do usuário), então a zona preferencial é a zona inicial para esse usuário.
- Se nem a aplicação nem o usuário tiverem uma associação de zona configurada, então a zona preferencial é a zona onde o usuário está executando uma instância do aplicativo Citrix Workspace (a localização do usuário). Se essa zona não estiver definida, uma seleção aleatória de VDA e zona é usada. O balanceamento de carga é aplicado a todos os VDAs na zona preferencial. Se não houver zona preferencial, o balanceamento de carga é aplicado a todos os VDAs no grupo de entrega.

Personalizando a preferência de zona

Ao configurar (ou remover) uma zona inicial para um usuário ou uma aplicação, você também pode restringir ainda mais como a preferência de zona é (ou não é) usada.

- **Uso obrigatório da zona inicial do usuário:** Em um grupo de entrega, você pode especificar "Iniciar a sessão na zona inicial do usuário (se o usuário tiver uma zona inicial), sem failover para uma zona diferente se os recursos não estiverem disponíveis na zona inicial." Essa restrição é útil se você quiser evitar o risco de copiar perfis grandes ou arquivos de dados entre zonas. Em outras palavras, você preferiria negar o início de uma sessão a iniciar a sessão em uma zona diferente.
- **Uso obrigatório da zona inicial da aplicação:** Da mesma forma, ao configurar uma zona inicial para uma aplicação, você pode especificar "iniciar a aplicação apenas nessa zona, sem failover para uma zona diferente se os recursos não estiverem disponíveis na zona inicial da aplicação."
- **Nenhuma zona inicial da aplicação e ignorar a zona inicial do usuário configurada:** Se você não especificar uma zona inicial para uma aplicação, também pode especificar "não considerar nenhuma zona de usuário configurada ao iniciar essa aplicação." Por exemplo, use a preferência de zona de localização do usuário se quiser que os usuários executem uma aplicação específica em um VDA próximo à sua máquina, mesmo que alguns usuários possam ter uma zona inicial diferente.

Como as zonas preferenciais afetam o uso da sessão

Quando um usuário inicia uma aplicação ou desktop, o broker prefere usar a zona preferencial em vez de usar uma sessão existente.

Se o usuário que inicia uma aplicação ou desktop já tiver uma sessão adequada para o recurso que está sendo iniciado (por exemplo, pode usar o compartilhamento de sessão para uma aplicação, ou uma sessão já executando o recurso que está sendo iniciado), mas essa sessão estiver em um VDA em uma zona diferente da zona preferencial para o usuário/aplicação, então o sistema pode criar uma nova sessão. Essa ação satisfaz o início na zona correta (se tiver capacidade disponível), antes de reconectar a uma sessão em uma zona menos preferencial para os requisitos de sessão desse usuário.

Para evitar uma sessão órfã que não pode mais ser alcançada, a reconexão é permitida para sessões desconectadas existentes, mesmo que estejam em uma zona não preferencial.

A ordem de desejabilidade para as sessões satisfazerem um lançamento é:

1. Reconectar a uma sessão existente na zona preferencial.
2. Reconectar a uma sessão desconectada existente em uma zona não preferencial.
3. Iniciar uma nova sessão na zona preferencial.
4. Reconectar a uma sessão existente conectada em uma zona não preferencial.

5. Iniciar uma nova sessão em uma zona não preferencial.

Outras considerações sobre a preferência de zona

- Se você configurar uma zona inicial para um grupo de usuários (como um grupo de segurança), os usuários desse grupo (por meio de associação direta ou indireta) serão associados à zona especificada. No entanto, um usuário pode ser membro de vários grupos de segurança e, portanto, pode ter uma zona inicial diferente configurada por meio de outra associação de grupo. Nesses casos, a determinação da zona inicial desse usuário pode ser ambígua.

  Se um usuário tiver uma zona inicial configurada que não foi adquirida por meio de associação a grupo, essa zona será usada para preferência de zona. Quaisquer associações de zona adquiridas por meio de associação a grupo são ignoradas.

  Se o usuário tiver várias associações de zona diferentes adquiridas exclusivamente por meio de associação a grupo, o broker escolherá aleatoriamente entre as zonas. Depois que o broker fizer essa escolha, essa zona será usada para lançamentos de sessão subsequentes, até que a associação do usuário ao grupo mude.
- A preferência de zona de localização do usuário requer a detecção do aplicativo Citrix Workspace no dispositivo de endpoint pelo Citrix Gateway através do qual esse dispositivo está se conectando. O Citrix deve ser configurado para associar intervalos de endereços IP a zonas específicas. A identidade da zona descoberta deve ser passada do StoreFront para o Citrix DaaS.

Embora escrito para o uso local de zonas, o post do blog Zone Preference Internals contém detalhes técnicos relevantes.

Permissões para gerenciar zonas

Um Administrador Completo pode executar todas as tarefas de gerenciamento de zona suportadas. Mover itens entre zonas não requer permissões relacionadas à zona (exceto permissão de leitura de zona). No entanto, você deve ter permissão de edição para os itens que está movendo. Por exemplo, para mover um catálogo de máquinas de uma zona para outra, você deve ter permissão de edição para esse catálogo.

Se você usa o Citrix Provisioning™: O console atual do Citrix Provisioning não tem conhecimento de zonas, então a Citrix recomenda usar o Studio para criar catálogos de máquinas que você deseja colocar em zonas específicas. Depois de criar o catálogo, você pode usar o console do Citrix Provisioning para provisionar máquinas nesse catálogo.

Criação de zona

Ao criar um local de recurso no Citrix Cloud e, em seguida, adicionar um Cloud Connector a esse local de recurso, o Citrix DaaS cria e nomeia automaticamente uma zona. Você pode, opcionalmente, adicionar uma descrição mais tarde.

Depois de criar mais de um local de recurso (e as zonas são criadas automaticamente), você pode mover recursos de uma zona para outra.

Os locais de recursos e as zonas são sincronizados periodicamente, geralmente e aproximadamente a cada cinco minutos. Assim, se você alterar o nome de um local de recurso no Citrix Cloud, essa alteração será propagada para a zona associada em cinco minutos.

Adicionar ou alterar uma descrição de zona

Embora você não possa alterar o nome de uma zona, você pode adicionar ou alterar sua descrição.

1. No Studio, selecione **Zonas** no painel esquerdo.
2. Selecione uma zona no painel central e, em seguida, selecione **Editar Zona** na barra de ações.
3. Adicione ou altere a descrição da zona.
4. Selecione **Salvar** ou **Aplicar.**

Atribuir escopos a uma zona

Atribua escopos a uma zona para conceder aos administradores personalizados acesso com escopo a zonas específicas. O controle de escopo ajuda você a alinhar o acesso administrativo com os requisitos operacionais e de segurança da sua organização.

Para atribuir escopos a uma zona, você deve ter a permissão **Editar escopo da zona**.

1. No Studio, selecione **Zonas** no painel esquerdo.
2. Selecione uma zona no painel central e, em seguida, selecione **Editar Zona** na barra de ações.
3. Selecione os escopos que você deseja atribuir à zona.
4. Se a caixa de seleção **Ignorar controle de escopo para este recurso** estiver selecionada, a zona estará visível para todos os administradores. Para aplicar o controle de escopo, desmarque a caixa de seleção e, em seguida, selecione os escopos desejados.
5. Selecione **Salvar** ou **Aplicar.**

Mover recursos de uma zona para outra zona

1. No Studio, selecione **Zonas** no painel esquerdo.
2. Selecione uma zona no painel do meio e, em seguida, selecione um ou mais itens.
3. Arraste os itens para a zona de destino ou selecione **Mover Itens** na barra de ações e, em seguida, especifique para qual zona movê-los. (Embora você possa selecionar Cloud Connectors, não é possível movê-los para uma zona diferente.)

Uma mensagem de confirmação lista os itens selecionados e pergunta se você tem certeza de que deseja mover todos eles.

Lembre-se: quando um catálogo de máquinas usa uma conexão de host com um hipervisor ou serviço de nuvem, certifique-se de que o catálogo e a conexão estejam na mesma zona. Caso contrário, o desempenho pode ser afetado. Se você mover um, mova o outro também.

Exclusão de zona

Você não pode excluir uma zona. No entanto, você pode excluir um local de recurso (depois de remover seus Cloud Connectors). A exclusão do local de recurso exclui automaticamente a zona.

- Se a zona não contiver nenhum item (como catálogos, conexões, aplicativos ou usuários), a zona será excluída durante a próxima sincronização entre zonas e locais de recursos. A sincronização ocorre a cada cinco minutos.
- Se a zona contiver itens, a zona será excluída automaticamente após a remoção de todos os itens.

Adicionar uma zona inicial para um usuário

Configurar uma zona inicial para um usuário também é conhecido como *adicionar um usuário a uma zona*.

1. No Studio, selecione **Zonas** no painel esquerdo.
2. Selecione uma zona no painel do meio e, em seguida, selecione **Adicionar Usuários à Zona** na barra de ações.
3. Na caixa de diálogo **Adicionar Usuários à Zona**, selecione **Adicionar** e, em seguida, selecione os usuários e grupos de usuários a serem adicionados à zona. Se você especificar usuários que já têm uma zona inicial, uma mensagem oferece duas opções: **Sim** = adicionar apenas os usuários especificados que não têm uma zona inicial; **Não** = retornar à caixa de diálogo de seleção de usuário.
4. Selecione **OK**.

Para usuários com uma zona inicial configurada, você pode exigir que as sessões sejam iniciadas apenas a partir de sua zona inicial:

1. Crie ou edite um grupo de entrega.
2. Na página **Usuários**, selecione a caixa de seleção **Exigir que as sessões sejam iniciadas na zona inicial de um usuário (se configurado)**.

Todas as sessões iniciadas por um usuário nesse grupo de entrega devem ser iniciadas a partir de máquinas na zona inicial desse usuário. Se um usuário no grupo de entrega não tiver uma zona inicial configurada, essa configuração não terá efeito.

Remover uma zona inicial para um usuário

Este procedimento também é conhecido como remover um usuário de uma zona.

1. No Studio, selecione **Zonas** no painel esquerdo.
2. Selecione uma zona no painel do meio e, em seguida, selecione **Remover Usuários da Zona** na barra de ações.
3. Na caixa de diálogo **Adicionar Usuários à Zona**, selecione **Remover** e, em seguida, selecione os usuários e grupos a serem removidos da zona. Esta ação remove os usuários apenas da zona. Esses usuários permanecem nos grupos de entrega aos quais pertencem.
4. Confirme a remoção quando solicitado.

Gerenciar zonas iniciais para aplicativos

Configurar uma zona inicial para um aplicativo também é conhecido como adicionar um aplicativo a uma zona. Por padrão, em um ambiente multizona, um aplicativo não tem uma zona inicial.

A zona inicial de um aplicativo é especificada nas propriedades do aplicativo. Você pode configurar as propriedades do aplicativo ao adicionar o aplicativo a um grupo ou posteriormente.

- Ao criar um grupo de entrega ou adicionar aplicativos a grupos existentes, selecione **Propriedades** na página **Aplicativos** do assistente.
- Para alterar as propriedades de um aplicativo depois que ele é adicionado, selecione **Zonas** no painel esquerdo. Selecione um aplicativo e, em seguida, selecione **Propriedades** na barra de ações.

Na página **Zonas** das propriedades/configurações do aplicativo:

- Se você quiser que o aplicativo tenha uma zona inicial:

    - Selecione o botão de opção **Usar a zona selecionada para decidir** e, em seguida, selecione a zona.
    - Se você quiser que o aplicativo seja iniciado apenas da zona selecionada (e não de qualquer outra zona), selecione a caixa de seleção abaixo da seleção de zona.

- Se você não quiser que o aplicativo tenha uma zona inicial:
    - Selecione o botão de opção **Não configurar uma zona inicial**.
    - Se você não quiser que o broker considere nenhuma zona de usuário configurada ao iniciar este aplicativo, selecione a caixa de seleção abaixo do botão de opção. Neste caso, nem as zonas iniciais do aplicativo nem as do usuário são usadas para determinar onde iniciar este aplicativo.

Outras ações que incluem a especificação de zonas

Se você tiver mais de uma zona, poderá especificar uma zona ao adicionar uma conexão de host ou criar um catálogo. As zonas são listadas em ordem alfabética nas listas de seleção. Por padrão, o primeiro nome alfabético é selecionado.

Solução de problemas

O Studio fornece alertas proativos para garantir que seu Local Host Cache e suas zonas estejam configurados corretamente, para que você possa resolver os problemas a tempo, antes que uma interrupção afete seus usuários. Esse recurso ajuda a manter o acesso contínuo do usuário a cargas de trabalho de missão crítica.

Uma guia **Solução de problemas** aparece para cada zona com problemas.

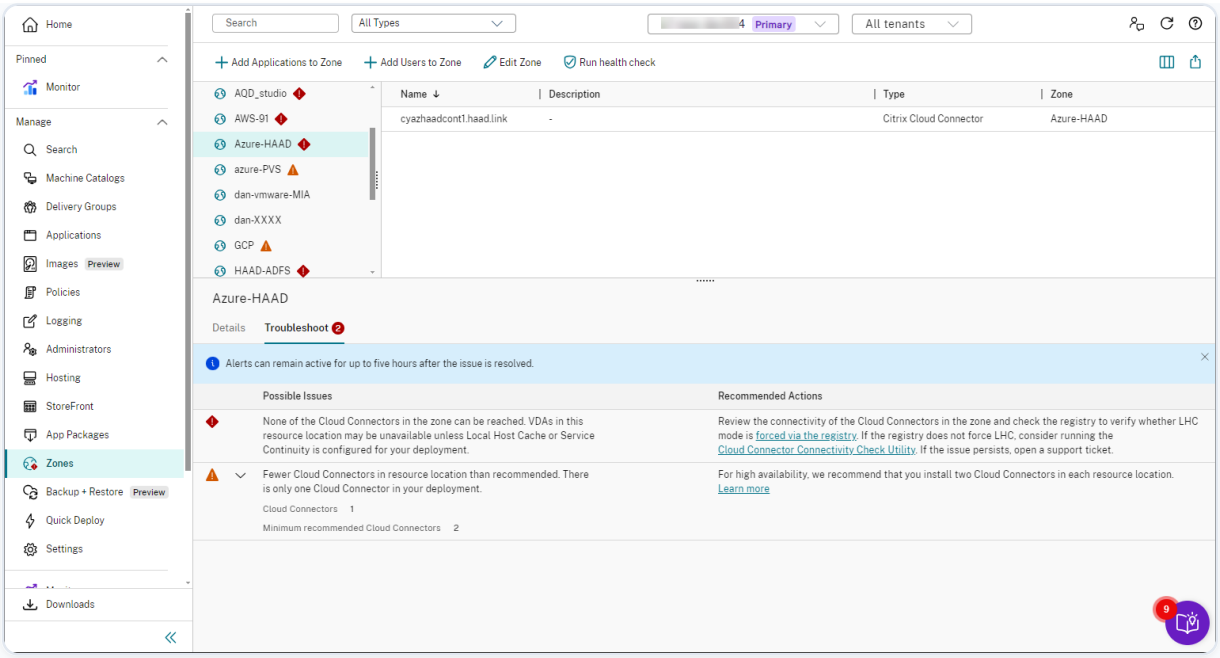
Para verificar problemas relacionados à zona, siga estas etapas:

1. Vá para **Zonas** e clique na zona com o ícone de aviso.
2. Vá para a guia **Solução de problemas** no painel inferior e leia as informações lá.

> **Nota:**

> Os diagnósticos são atualizados a cada hora.

> Exemplo de informações de solução de problemas:



A tabela a seguir fornece uma lista completa de avisos e erros relacionados à zona:

GRAVIDADE	POSSÍVEIS PROBLEMAS	AÇÕES RECOMENDADAS
Aviso	O local do recurso contém vários domínios. Locais de recursos que contêm vários domínios podem causar atrasos ou falhas nos registros de VDA quando no modo Local Host Cache.	Reconfigure seu local de recurso para que todos os Cloud Connectors estejam no mesmo domínio. Consulte os Detalhes Técnicos do Citrix Cloud Connector para obter mais informações sobre configurações multidomínio suportadas.
Aviso	O número de conexões de host no local do recurso excede o limite recomendado, o que pode resultar em degradação do desempenho.	Reduza o número de conexões de host no local do recurso para não mais do que o limite recomendado. Consulte Limites.
Aviso	Há apenas um Cloud Connector no local do recurso.	Para alta disponibilidade, instale dois Cloud Connectors em cada local de recurso. Consulte os Detalhes Técnicos do Citrix Cloud Connector.

GRAVIDADE	POSSÍVEIS PROBLEMAS	AÇÕES RECOMENDADAS
Aviso	Há menos CPUs por soquete do que o recomendado, o que pode resultar em degradação do desempenho no modo Local Host Cache.	Certifique-se de que cada Cloud Connector atenda aos requisitos mínimos de CPU por soquete. Consulte Configuração de computação recomendada para Local Host Cache.
Aviso	O StoreFront não está enviando solicitações STA para todos os Cloud Connectors neste local de recurso.	Certifique-se de que todos os Cloud Connectors sejam adicionados como servidores STA no StoreFront e no NetScaler® Gateway para evitar falhas de inicialização no modo Local Host Cache.
Aviso	O StoreFront é detectado no Local do Recurso, mas pelo menos um Connector dentro do Local do Recurso não está recebendo tráfego do StoreFront. A falta de tráfego do StoreFront pode afetar a escalabilidade e causar problemas ao entrar no modo de alta disponibilidade.	Certifique-se de que todos os Cloud Connectors estejam listados como um feed de recurso no StoreFront e verifique se o StoreFront pode se comunicar com todos os Connectors listados na porta especificada no feed de recurso.
Aviso	O local do recurso tem vários brokers de Local Host Cache eleitos. Ter vários brokers de Local Host Cache eleitos pode fazer com que os registros de VDA sejam divididos entre os conectores no modo Local Host Cache, levando a falhas intermitentes de inicialização.	Certifique-se de que os conectores possam se comunicar em `http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection`. Consulte Zonas com vários Cloud Connectors.
Aviso	Há menos processadores lógicos de CPU do que o recomendado, o que pode	Certifique-se de que cada Cloud Connector atenda aos requisitos mínimos de

GRAVIDADE	POSSÍVEIS PROBLEMAS	AÇÕES RECOMENDADAS
	resultar em degradação do desempenho no modo Local Host Cache.	processador lógico de CPU para o Local Host Cache. Consulte Configuração de computação recomendada para Local Host Cache.
Aviso	Há menos RAM do que o recomendado, o que pode resultar em degradação do desempenho no modo Local Host Cache.	Certifique-se de que cada Cloud Connector atenda aos requisitos mínimos de RAM para o Local Host Cache. Consulte Configuração de computação recomendada para Local Host Cache.
Erro	Há mais VDAs no local do recurso do que o recomendado, o que resultará em falhas de registro de VDA no modo Local Host Cache.	Reduza o número de VDAs neste local de recurso para não mais do que o limite recomendado. Consulte Limites.
Erro	Nenhum dos Cloud Connectors na zona pode ser alcançado. Os VDAs neste local de recurso devem estar disponíveis através do Local Host Cache ou Service Continuity.	Revise a conectividade dos Cloud Connectors na zona e verifique o registro para ver se o modo LHC é forçado via registro. Se o LHC não for forçado através do registro, considere executar o Utilitário de Verificação de Conectividade do Cloud Connector. Se o problema persistir, abra um tíquete de suporte.
Erro	Há menos processadores lógicos de CPU do que o recomendado, o que pode resultar em degradação do desempenho.	Certifique-se de que cada Cloud Connector atenda aos requisitos mínimos de processador lógico de CPU. Consulte Detalhes Técnicos do Citrix Cloud Connector.

GRAVIDADE	POSSÍVEIS PROBLEMAS	AÇÕES RECOMENDADAS
Erro	Há menos RAM do que o recomendado, o que pode resultar em degradação do desempenho.	Certifique-se de que cada Cloud Connector atenda aos requisitos mínimos de RAM. Consulte Detalhes Técnicos do Citrix Cloud Connector.

Para obter um relatório detalhado de configurações incorretas na zona, execute o cmdlet do PowerShell, `Get-ConfigMisconfigurationReport`. Os detalhes adicionados incluem informações como qual Connector está configurado incorretamente, qual é a configuração incorreta atual e qual é a configuração recomendada.

Remover usuário do broker do cache

Há casos em que os administradores não conseguem remover um usuário do broker do cache ou, às vezes, ao executar `Get-BrokerUser`, o usuário exibe o SID incorreto do AD.

Isso acontece quando o usuário é excluído do AD e recriado, mas o cache do broker ainda contém o SID do usuário anterior.

Para resolver isso, faça o seguinte:

1. Remova os usuários do Active Directory.
2. Execute `Get-BrokerUser` para cada conta removida. Contas que não são referenciadas em nenhum lugar não retornam resultados. Para usuários que são referenciados, você obtém um valor depois de executar `Get-BrokerUser`. Agora, você deve descobrir a quais recursos o usuário está atribuído e remover manualmente os usuários desses recursos.

   Por exemplo:

   - Verifique se o usuário está atribuído a um aplicativo: `Get-BrokerApplication`
   - Verifique se o usuário está atribuído a um grupo de aplicativos: `Get-BrokerApplicationGroup`
   - Verifique se o usuário está atribuído a uma política de acesso: `Get-BrokerAccessPolicyRule`
   - Verifique se o usuário está atribuído a uma política de direitos de aplicativo: `Get-BrokerAppEntitlementPolicyRule`

- Verifique se o usuário está atribuído a uma política de direitos de desktop: `Get-BrokerEntitlementPolicyRule`
- Verifique se o usuário está atribuído a uma sessão persistente de grupo de desktop: `Get-BrokerSessionLinger`
- Verifique se o usuário está executando alguma sessão em um VDA: `Get-BrokerSession`
- Verifique se o usuário está atribuído a um recurso no grupo mesclado: `Get-BrokerMergedResource`
- Verifique se o usuário está atribuído a um grupo de recursos: `Get-BrokerMergeGroup`
- Verifique se um comando está na fila para um usuário: `Get-BrokerMachineCommand`
- Verifique se o usuário está atribuído a um desktop privado: `Get-BrokerMachineV2`
- Verifique se o usuário está atribuído a uma preferência de zona: `Get-BrokerUserZonePreference`

3. Remova manualmente os usuários dos recursos.
4. Execute o comando `Get-BrokerUser` para confirmar que o usuário foi removido de todos os recursos.
5. Depois que o usuário for removido de todos os recursos, execute o seguinte para remover o usuário do cache.

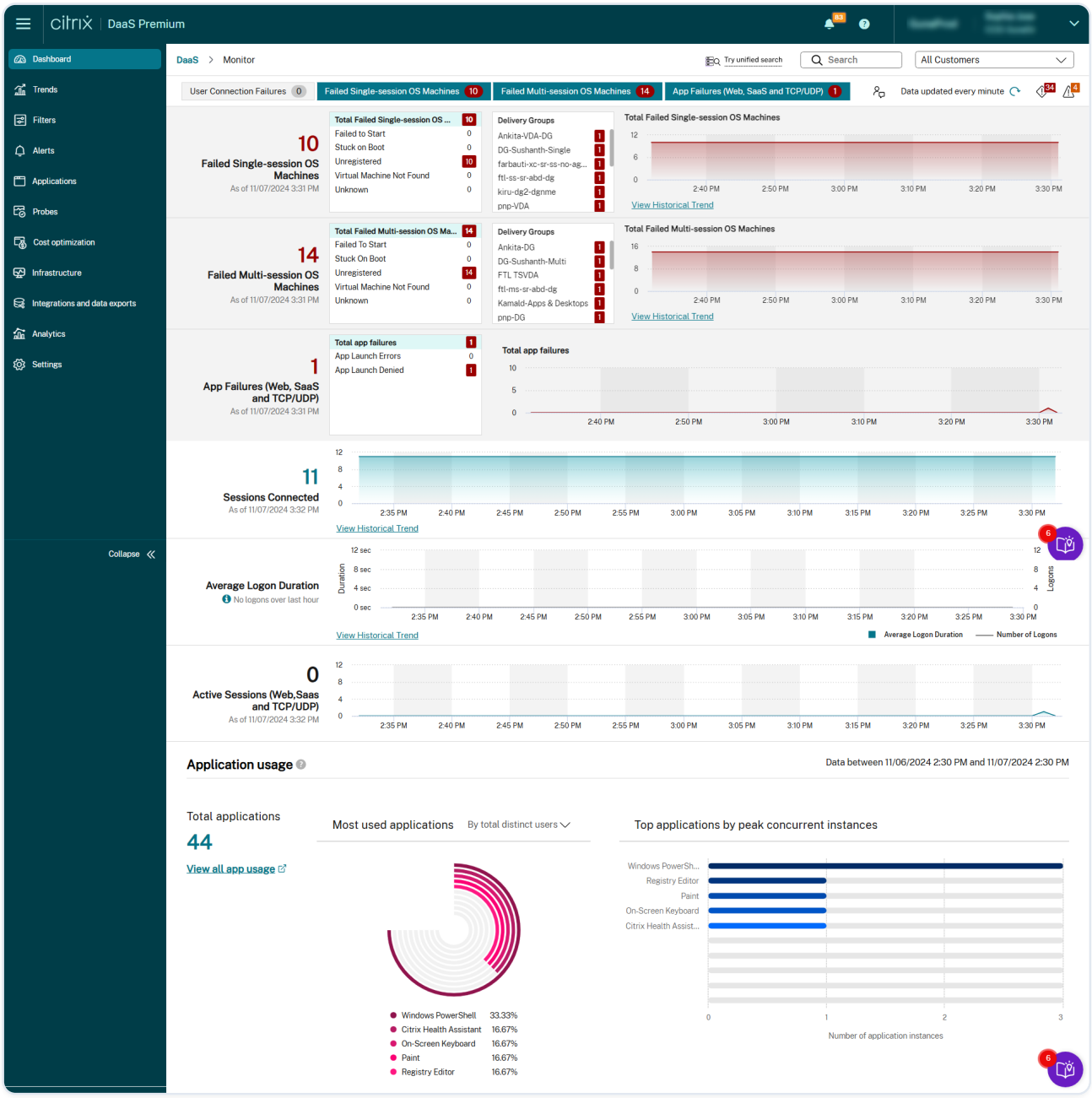
```
Update-BrokerNameCache -Users -Purge -UnusedFor 0
```

Monitor

Administradores e pessoal de suporte técnico podem monitorar o Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™) a partir do **Monitor**, o console de monitoramento e solução de problemas. O nó **Monitor** direciona você para um painel para monitorar, solucionar problemas e executar tarefas de suporte para assinantes.

> **Nota:**
>
> O Monitor está disponível como o console do Director para monitorar e solucionar problemas de implantações do Citrix Virtual Apps and Desktops Current Release e LTSR.

> Para acessar o **Monitor**, faça login no Citrix Cloud. No menu superior esquerdo, selecione **Soluções > DaaS**. Clique em **Monitor**.



Nota:

A resolução de tela ideal recomendada para visualizar o Citrix Monitor é 1440 x 1024.

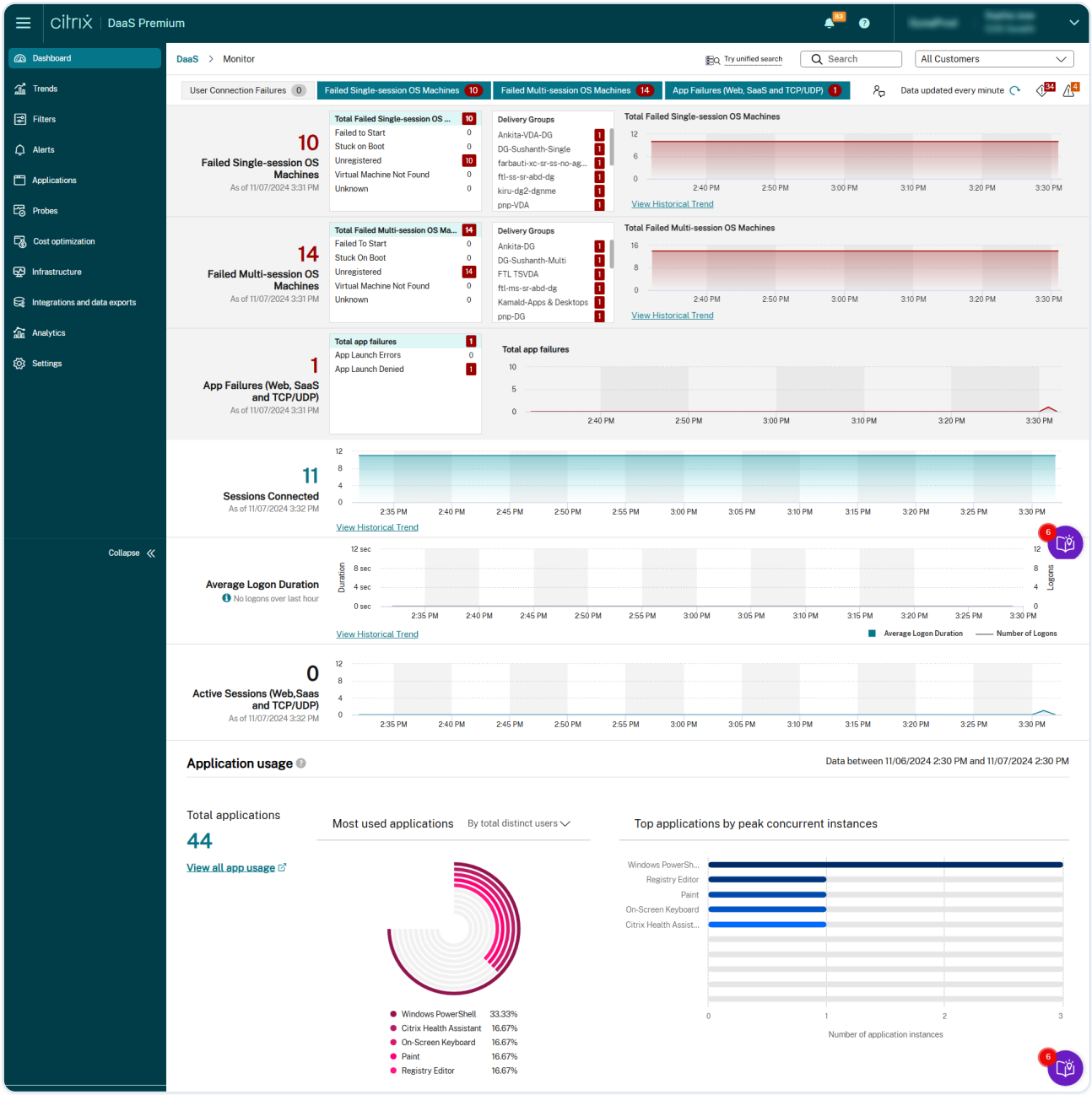
O Monitor oferece:

- Dados em tempo real do Broker Agent usando um console unificado integrado com o Analytics e o Performance Manager.
- O Analytics inclui gerenciamento de desempenho para garantia de saúde e capacidade, e tendências históricas para identificar gargalos em seu ambiente Citrix DaaS™.

- Dados históricos armazenados no banco de dados do Monitor para acessar o banco de dados de Log de Configuração.
- Obtenha visibilidade da experiência do usuário final para aplicativos virtuais, desktops e usuários para Citrix DaaS.
- O Monitor usa um painel de solução de problemas que fornece monitoramento de saúde em tempo real e histórico do Citrix DaaS. Este recurso permite que você veja falhas em tempo real, proporcionando uma ideia melhor do que os usuários finais estão experimentando.

Análise do site

O painel do Monitor fornece um local centralizado para monitorar a integridade e o uso de um site.



Se não houver falhas atualmente e nenhuma falha tiver ocorrido nos últimos 60 minutos, os painéis permanecerão recolhidos. Quando houver falhas, o painel de falha específico aparecerá automaticamente.

PAINEL	DESCRIÇÃO
Falhas de Conexão do Usuário	Falhas de conexão nos últimos 60 minutos. Clique nas categorias ao lado do número total para visualizar as métricas para esse tipo de falha. Na tabela adjacente, esse número é categorizado ainda mais com base em cada grupo de entrega. As falhas de conexão incluem falhas causadas pelo atingimento dos limites do aplicativo. Para obter mais informações sobre os limites do aplicativo, consulte Aplicativos.
Máquinas OS de sessão única com falha ou Máquinas OS de várias sessões com falha	Total de falhas nos últimos 60 minutos, categorizadas com base em cada grupo de entrega. Falhas divididas por tipos, incluindo falha ao iniciar, travado na inicialização e não registrado. Para máquinas OS de várias sessões, as falhas também incluem máquinas que atingem a carga máxima.
Sessões Conectadas	Sessões conectadas em todos os grupos de entrega nos últimos 60 minutos.
Duração Média do Logon	Dados de logon dos últimos 60 minutos. O número grande à esquerda é a duração média do logon ao longo da hora. Os dados de logon para VDAs anteriores ao XenDesktop 7.0 não estão incluídos nesta média. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.
Total de usuários conectados	Mostra o número de usuários que tiveram pelo menos uma conexão nas últimas 24 horas ou nos últimos 7 dias. Este painel ajuda os administradores a apresentar as tendências de adoção aos seus executivos.

PAINEL	DESCRIÇÃO
Versões do aplicativo Citrix Workspace™ encontradas em seu ambiente	Fornece uma visão geral das versões do aplicativo Citrix Workspace usadas em toda a organização. Ajuda a unificar as versões mostrando quantos dispositivos estão usando versões diferentes. Por padrão, os dados da versão do aplicativo Citrix Workspace para todas as plataformas de SO são exibidos. Você pode visualizar os dados da versão para uma plataforma de SO específica selecionando o SO correspondente na lista suspensa **Plataforma**.

> **Nota:**
>
> Quando o tipo de host que você está usando não suporta uma métrica específica, nenhum ícone aparece para essa métrica. Por exemplo, nenhuma informação de saúde está disponível para hosts do System Center Virtual Machine Manager (SCVMM), AWS e CloudStack.

> Continue a solucionar problemas usando estas opções (que estão documentadas nas seções anteriores):

- Controlar energia da máquina do usuário
- Impedir conexões com máquinas

Monitorar sessões

Se uma sessão for desconectada, ela ainda estará ativa e seus aplicativos continuarão a ser executados. No entanto, o dispositivo do usuário não estará mais se comunicando com o servidor.

AÇÃO	DESCRIÇÃO
Visualizar a máquina ou sessão atualmente conectada de um usuário	Nas exibições Gerenciador de Atividades e Detalhes do Usuário, visualize a máquina ou sessão atualmente conectada do usuário. Além disso, visualize uma lista de todas as máquinas e sessões às quais este usuário tem

AÇÃO	DESCRIÇÃO
	acesso. Para acessar esta lista, clique no ícone do alternador de sessão na barra de título do usuário. Para obter mais informações, consulte Restaurar sessões.
Visualizar o número total de sessões conectadas em todos os grupos de entrega	No Painel, no painel **Sessões Conectadas**, visualize o número total de sessões conectadas em todos os grupos de entrega nos últimos 60 minutos. Em seguida, clique no grande número total, que abre a visualização Filtros. Aqui, você pode exibir dados gráficos de sessão com base nos grupos de entrega e intervalos selecionados e no uso em todos os grupos de entrega.
Encerrar sessões ociosas	A visualização Filtros de Sessões exibe dados relacionados a todas as sessões ativas. Você pode filtrar as sessões com base no Usuário Associado, grupo de entrega, Estado da Sessão e Tempo Ocioso maior que um período de tempo limite. Na lista filtrada, selecione as sessões para fazer logoff ou desconectar. Para obter mais informações, consulte Solucionar problemas de aplicativos.
Visualizar dados por um período mais longo	Na visualização **Tendências**, selecione a guia **Sessões** para detalhar dados de uso mais específicos. Você pode detalhar dados para sessões conectadas e desconectadas por um período mais longo. Você pode visualizar os totais de sessões de antes dos últimos 60 minutos. Para visualizar essas informações, clique em **Visualizar tendências históricas**.

Nota:

Considere que um dispositivo de usuário esteja executando um Virtual Delivery Agent (VDA) legado, como um VDA anterior à versão 7, ou um VDA Linux. Nesse caso, o Monitor não

> pode exibir informações completas sobre a sessão. Em vez disso, ele exibe uma mensagem de que as informações não estão disponíveis.

> **Limitação das Regras de Atribuição de Desktop:** O Studio permite a atribuição de várias Regras de Atribuição de Desktop (DAR) para diferentes usuários ou grupos de usuários a um único VDA no grupo de entrega. O StoreFront™ exibe o desktop atribuído com o **Nome de Exibição** correspondente de acordo com a DAR para o usuário logado. No entanto, o Monitor não oferece suporte a DARs e exibe o desktop atribuído usando o nome do grupo de entrega, independentemente do usuário logado. Como resultado, você não pode mapear um desktop específico para uma máquina no Monitor.

Você pode mapear o desktop atribuído que é exibido no StoreFront para o nome do grupo de entrega que é exibido no Monitor. Para o mapeamento, use o seguinte comando PowerShell:

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

Execute o comando PowerShell anterior usando o SDK do Remote PowerShell conforme descrito no blog.

Desabilitar a visibilidade de aplicativos em execução no Gerenciador de Atividades

Por padrão, o Gerenciador de Atividades exibe uma lista de todos os aplicativos em execução para a sessão de um usuário. Todos os administradores que têm acesso ao recurso Gerenciador de Atividades podem visualizar essas informações. Para funções de Administrador Delegado, esta visualização inclui Administrador Completo, Administrador de grupo de entrega e Administrador de Help Desk.

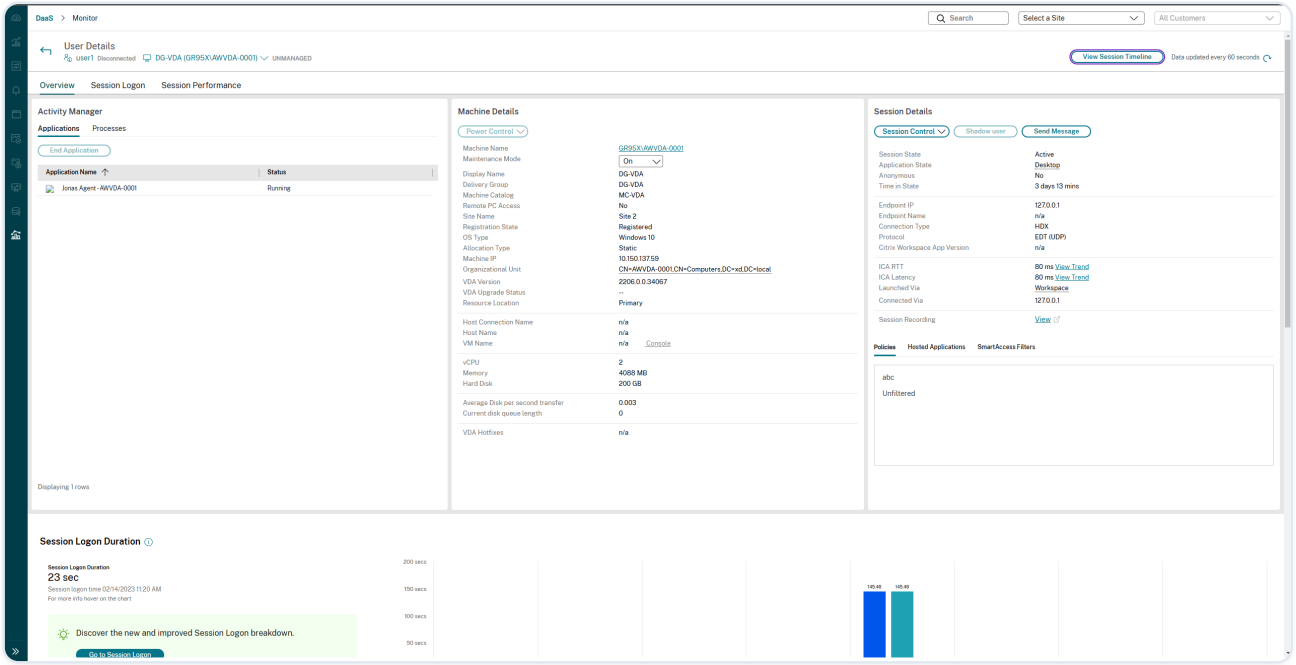
Para proteger a privacidade dos usuários e dos aplicativos que eles estão executando, você pode desabilitar a guia **Aplicativos** para listar os aplicativos em execução. Para realizar esta atividade, no VDA, modifique a chave do registro em `HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed`. Por padrão, a chave é definida como 1. Altere o valor para 0, o que significa que as informações não são coletadas do VDA e, como tal, não são exibidas no Gerenciador de Atividades.

> **Aviso:**

A edição incorreta do registro pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Acessar Citrix Analytics for Performance™ - Detalhes da Sessão

A página Detalhes da Sessão do Citrix Analytics for Performance pode ser acessada no Monitor. Clicar em **Visualizar Linha do Tempo da Sessão** na seção **Detalhes da Sessão** do Gerenciador de Atividades abre a página Detalhes da Sessão do Citrix Analytics for Performance dentro do Monitor.

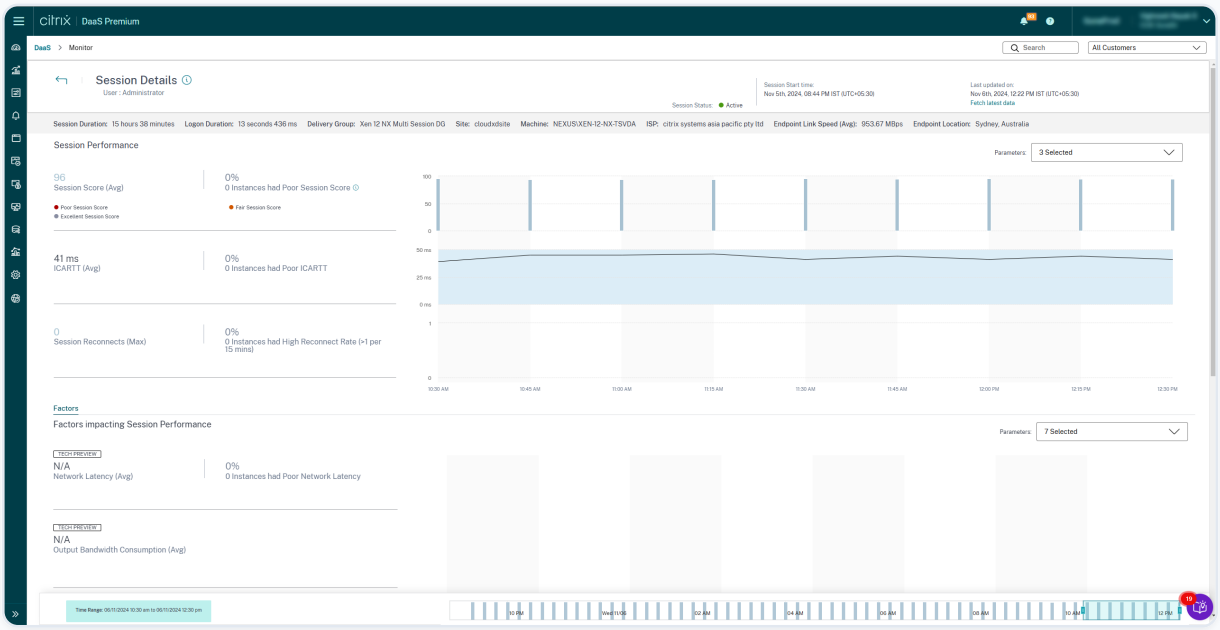


Nota:

Este recurso exige que você tenha um direito válido ao Citrix Analytics for Performance.

Os Detalhes da Sessão estão disponíveis para sessões categorizadas como Excelente, Razoável ou Ruim no Citrix Analytics for Performance. Para obter mais informações sobre os motivos pelos quais uma sessão pode não ser categorizada, consulte o artigo Não

Categorizado.

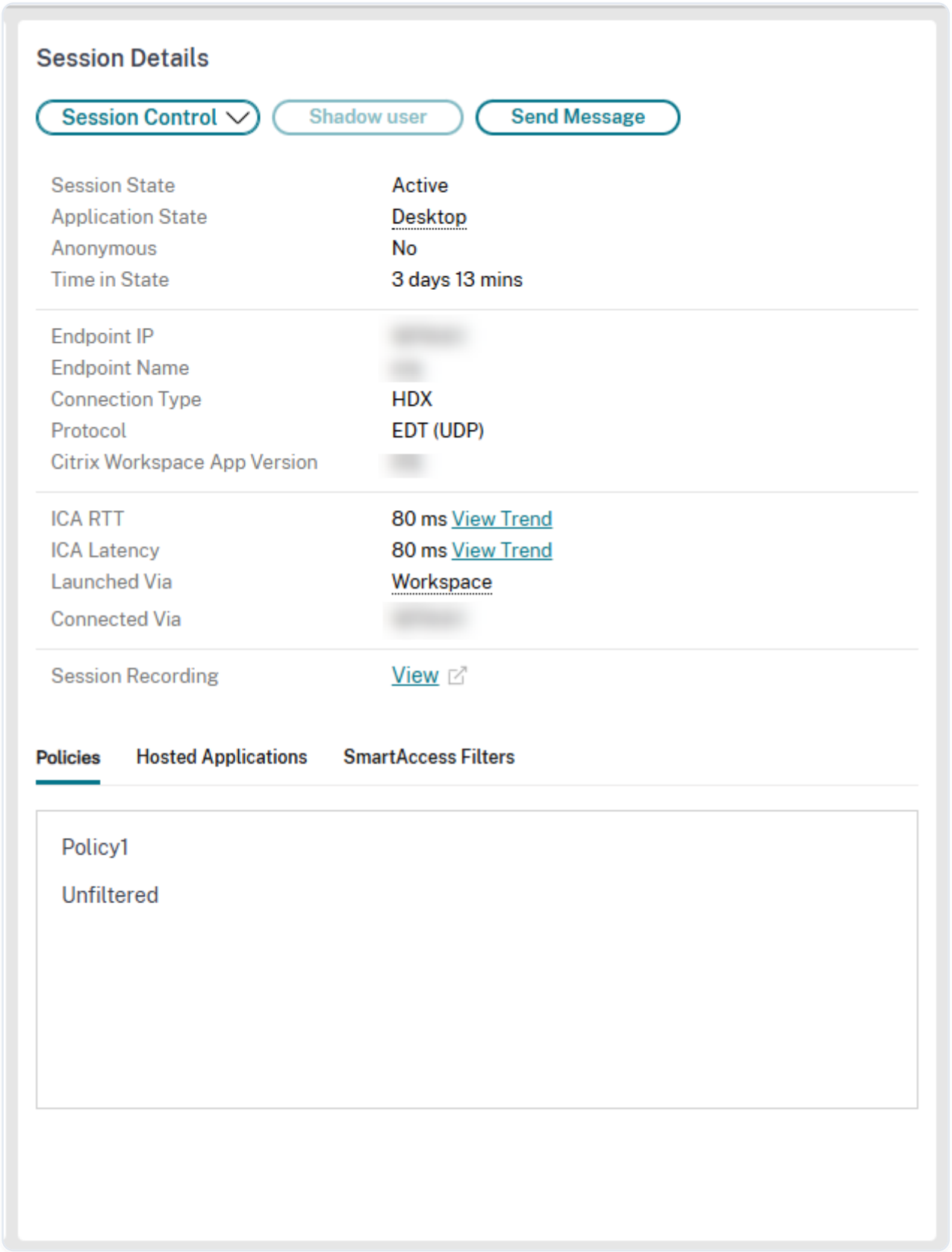


Você pode visualizar uma tendência da experiência da sessão para a sessão por até os últimos três dias. Esta visualização de tendência também inclui os fatores que contribuem para a experiência da sessão. Esta informação complementa os dados em tempo real disponíveis no Monitor, usados pelo administrador do suporte técnico ao solucionar problemas relacionados à experiência da sessão.

Para obter mais informações sobre a página Detalhes da Sessão, consulte Detalhes da Sessão.

Protocolo de transporte da sessão

Visualize o protocolo de transporte em uso para o tipo de conexão HDX para a sessão atual no painel **Detalhes da Sessão**. Esta informação está disponível para sessões iniciadas em VDAs Versão 7.13 ou posterior.



Use o menu suspenso **Controle de Sessão** no painel **Detalhes da Sessão** para fazer logoff ou desconectar uma sessão.

- Para o tipo de conexão **HDX™**,
  - O Protocolo é exibido como **UDP**, se o EDT for usado para a conexão HDX.

    - O Protocolo é exibido como **TCP**, se o TCP for usado para a conexão HDX.

- Para o tipo de conexão **RDP**, o Protocolo é exibido como **n/a**.

Quando o transporte adaptativo é configurado, o protocolo de transporte da sessão alterna dinamicamente entre EDT (sobre UDP) e TCP, com base nas condições da rede. Se a sessão HDX não puder ser estabelecida usando EDT, ela retornará ao protocolo TCP.

Para obter mais informações sobre a configuração do transporte adaptativo, consulte Transporte Adaptativo.

Exportar relatórios

Você pode exportar dados de tendências para gerar relatórios regulares de uso e gerenciamento de capacidade. A exportação suporta os formatos de relatório PDF, Excel e CSV. Relatórios nos formatos PDF e Excel incluem tendências representadas como gráficos e tabelas. Relatórios no formato CSV contêm dados tabulares que você pode usar para gerar visualizações ou para arquivar.

Para exportar um relatório:

1. Vá para a guia **Tendências**.
2. Defina os critérios de filtro e o período e clique em **Aplicar**. O gráfico de tendências e a tabela são preenchidos com dados.
3. Clique em **Exportar** e insira o nome e o formato do relatório.

O Monitor gera o relatório com base nos critérios de filtro que você seleciona. Se você alterar os critérios de filtro, clique em **Aplicar** antes de clicar em **Exportar**.

> **Nota:**
>
> A exportação de uma grande quantidade de dados causa um aumento significativo no consumo de memória e CPU no servidor Monitor, no Delivery Controller™ e nos servidores SQL. O número suportado de operações de exportação simultâneas e a quantidade de dados que podem ser exportados são definidos para limites padrão para obter um desempenho de exportação ideal.

Limites de exportação suportados

Os relatórios PDF e Excel exportados contêm gráficos completos para os critérios de filtro selecionados. No entanto, os dados tabulares em todos os formatos de relatório são truncados além dos limites padrão no número de linhas ou registros na tabela. O número padrão de registros suportados é definido com base no formato do relatório.

FORMATO DO RELATÓRIO	NÚMERO PADRÃO DE REGISTROS SUPORTADOS
PDF	500
Excel	100.000
CSV	100.000 (10.000.000 na guia **Sessões**)

Tratamento de Erros

Erros que você pode encontrar durante uma operação de Exportação:

- **O Director atingiu o tempo limite:** Este erro pode ocorrer devido a problemas de rede ou alto uso de recursos no servidor Director ou com o Serviço de Monitoramento.
- **O Monitor atingiu o tempo limite:** Este erro pode ocorrer devido a problemas de rede ou alto uso de recursos com o Serviço de Monitoramento ou no servidor SQL.
- **Máximo de operações de Exportação ou Visualização simultâneas em andamento:** Apenas uma instância de Exportação ou Visualização pode ser executada por vez. Se você receber o erro **Máximo de operações de Exportação ou Visualização simultâneas em andamento**, tente a próxima operação novamente mais tarde.

Hotfixes do Monitor

Para visualizar os hotfixes instalados em um VDA de máquina específico (físico ou VM), escolha a exibição **Detalhes da Máquina**.

Controlar estados de energia da máquina do usuário

Para controlar o estado das máquinas que você seleciona no Monitor, use as opções de Controle de Energia. Essas opções estão disponíveis para máquinas de SO de sessão única, mas podem não estar disponíveis para máquinas de SO de múltiplas sessões.

> **Nota:**

Esta funcionalidade não está disponível para máquinas físicas ou máquinas que usam o Acesso Remoto ao PC.

COMANDO	FUNÇÃO
Reiniciar	Executa um desligamento ordenado (suave) da VM e todos os processos em execução são interrompidos individualmente antes de reiniciar a VM. Por exemplo, selecione as máquinas que aparecem no Monitor como "falha ao iniciar" e use este comando para reiniciá-las.
Forçar Reinício	Reinicia a VM sem primeiro executar qualquer procedimento de desligamento. Este comando funciona da mesma forma que desconectar um servidor físico e depois conectá-lo novamente e ligá-lo.
Desligar	Executa um desligamento ordenado (suave) da VM. Todos os processos em execução são interrompidos individualmente.
Forçar Desligamento	Desliga a VM sem primeiro executar qualquer procedimento de desligamento. Este comando funciona da mesma forma que desconectar um servidor físico. Pode nem sempre desligar todos os processos em execução, e você corre o risco de perder dados se desligar uma VM dessa maneira.
Suspender	Suspende uma VM em execução em seu estado atual e armazena esse estado em um arquivo no repositório de armazenamento padrão. Esta opção permite que você desligue o servidor host da VM e, posteriormente, após reiniciá-lo,

COMANDO	FUNÇÃO
	retome a VM, retornando-a ao seu estado de execução original.
Retomar	Retoma uma VM suspensa e restaura seu estado de execução original.
Iniciar	Inicia uma VM quando ela está desligada (também conhecido como inicialização a frio).

Se as ações de controle de energia falharem, passe o mouse sobre o alerta e uma mensagem pop-up aparecerá com detalhes sobre a falha.

Impedir conexões a máquinas

Use o modo de manutenção para impedir novas conexões temporariamente enquanto o administrador apropriado executa tarefas de manutenção na imagem.

Quando você habilita o modo de manutenção nas máquinas, nenhuma nova conexão é permitida até que você o desabilite. Se os usuários estiverem atualmente logados, o modo de manutenção entra em vigor quando todos os usuários fazem logoff. Para usuários que não fazem logoff, envie uma mensagem informando-os de que as máquinas serão desligadas em um determinado horário. Você pode usar os controles de energia para forçar o desligamento das máquinas.

1. Selecione a máquina, como na exibição Detalhes do Usuário, ou um grupo de máquinas na exibição Filtros.
2. Selecione **Modo de Manutenção** e ative a opção.

Se um usuário tentar se conectar a um desktop atribuído enquanto ele estiver no modo de manutenção, uma mensagem aparecerá para indicar que o desktop está indisponível. Nenhuma nova conexão poderá ser feita até que você desabilite o modo de manutenção.

Análise de Aplicativos

A guia **Aplicativos** exibe análises baseadas em aplicativos em uma exibição única e consolidada para ajudar a analisar e gerenciar o desempenho do aplicativo de forma eficiente. Você pode obter informações valiosas sobre a integridade e o uso de todos os aplicativos publicados no site. Ele mostra métricas como as seguintes:

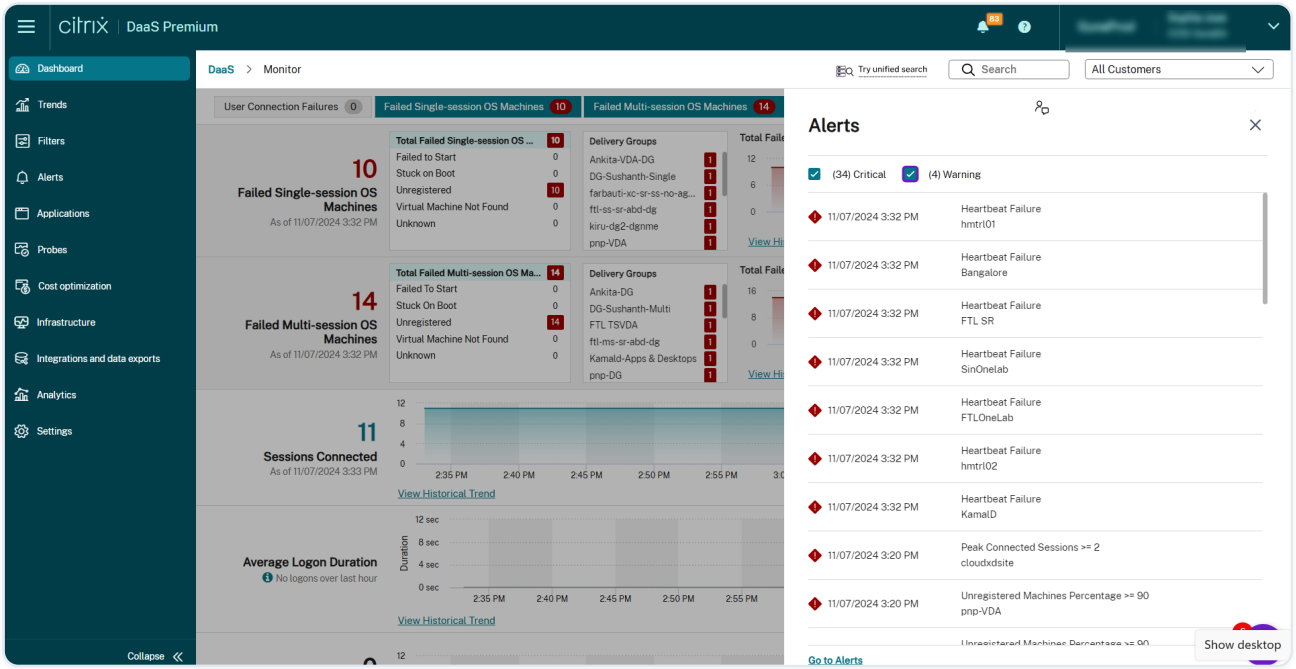
- Resultados da sondagem

- Número de instâncias por aplicativo
- Falhas e erros associados aos aplicativos publicados

Para obter mais informações, consulte a seção Análise de Aplicativos em **Solução de Problemas de Aplicativos**.

Alertas e notificações

Os alertas são exibidos no Monitor no painel e em outras visualizações de alto nível com símbolos de alerta de aviso e crítico. Os alertas são atualizados automaticamente a cada minuto; você também pode atualizar os alertas sob demanda.

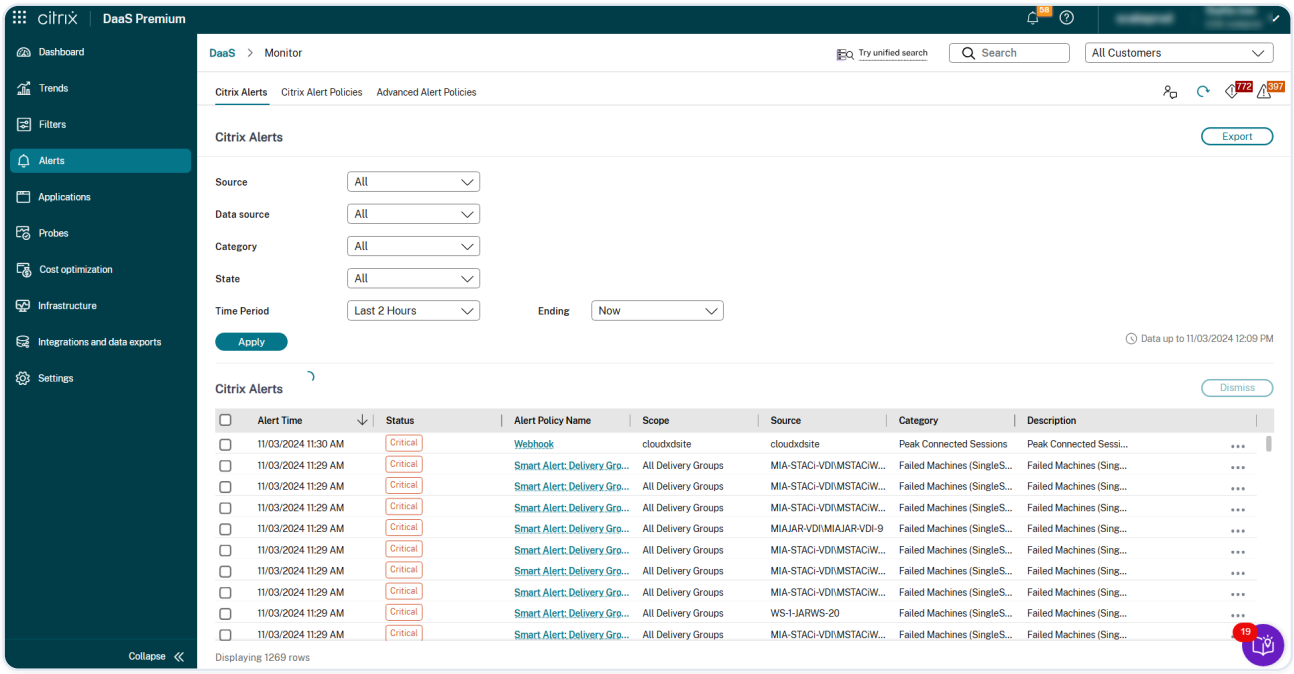


Um alerta de aviso (triângulo âmbar) indica que o limite de aviso de uma condição foi atingido ou excedido.

Um alerta crítico (círculo vermelho) mostra que o limite crítico de uma condição foi atingido ou excedido.

Você pode visualizar informações mais detalhadas sobre os alertas selecionando um alerta na barra lateral, clicando no link **Ir para Alertas** na parte inferior da barra lateral ou selecionando **Alertas** na parte superior da página Monitor.

Na visualização Alertas, você pode filtrar e exportar alertas. Por exemplo, máquinas Multi-session OS com falha para um grupo de entrega específico no último mês, ou todos os alertas para um usuário específico. Para obter mais informações, consulte Exportar relatórios.



Alertas Citrix®

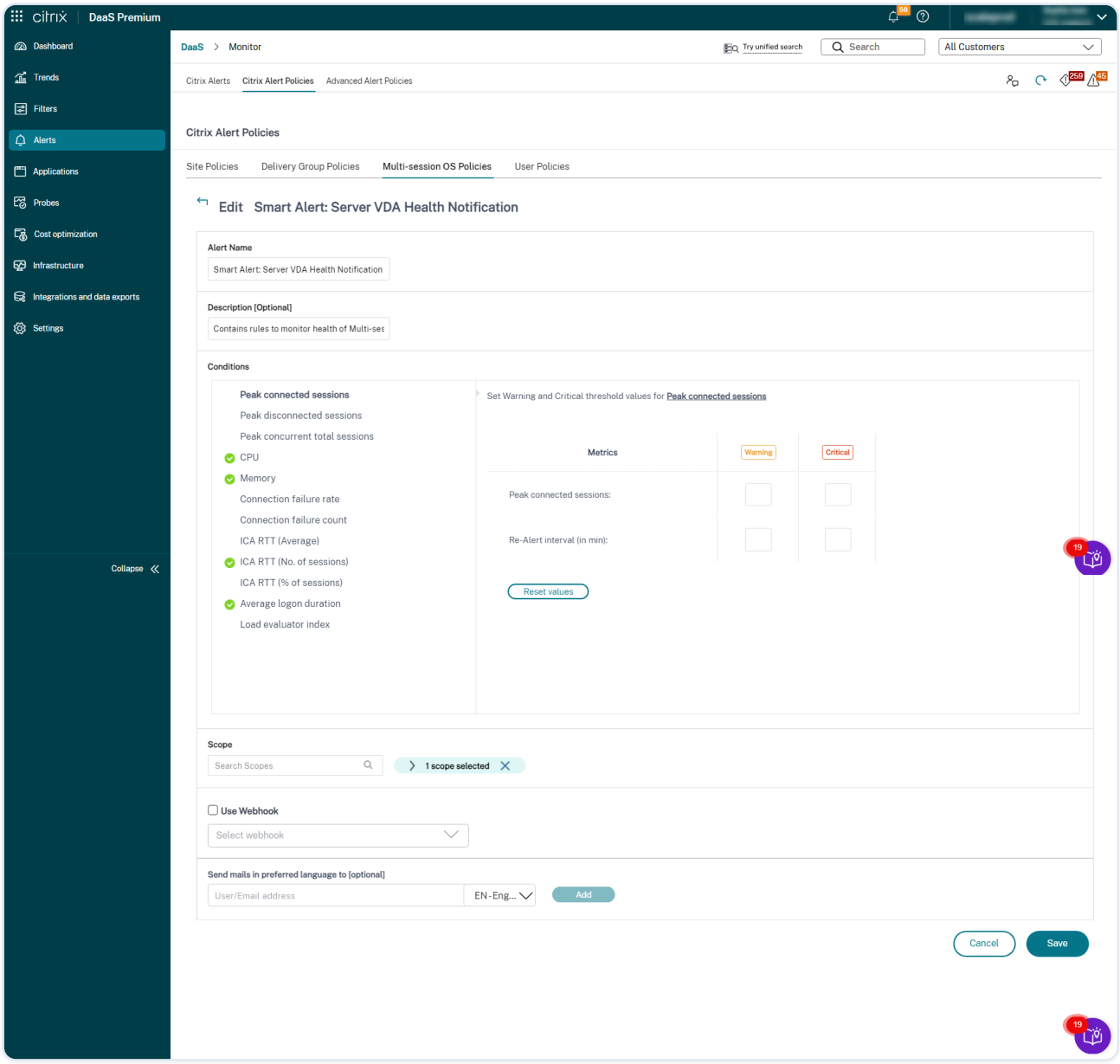
Os alertas Citrix são aqueles que se originam dos componentes Citrix. Você pode configurar alertas Citrix dentro do Monitor em **Alertas** \> **Política de Alertas Citrix**. Como parte da configuração, você pode definir notificações a serem enviadas por e-mail para indivíduos e grupos quando os alertas excederem os limites que você configurou. Para obter mais informações sobre como configurar Alertas Citrix, consulte Criar políticas de alerta.

Políticas de alerta inteligentes

Um conjunto de políticas de alerta integradas com valores de limite predefinidos está disponível para grupos de entrega e escopo de VDAs de SO de múltiplas sessões. Você pode modificar os parâmetros de limite das políticas de alerta integradas em **Alertas** \> **Política de Alertas Citrix**. Essas políticas são criadas quando há pelo menos um destino de alerta — um grupo de entrega ou um VDA de SO de múltiplas sessões definido em seu site. Além disso, esses alertas integrados são adicionados automaticamente a um novo grupo de entrega ou a um VDA de SO de múltiplas sessões.

As políticas de alerta integradas são criadas somente se nenhuma regra de alerta correspondente existir no banco de dados do Monitor.

Para os valores de limite das políticas de alerta integradas, consulte a seção Condições das políticas de alerta.



Políticas de alerta avançadas

O recurso de Notificação e Alerta Proativo do Monitor foi aprimorado para incluir uma nova estrutura de alerta chamada **Políticas de Alerta Avançadas**. Com esse recurso, você pode criar alertas incluindo detalhes granulares para cada elemento ou condição, aumentando assim o controle sobre o escopo dos alertas. Atualmente, essas políticas incluem alertas para economia de custos e infraestrutura.

Com a introdução das políticas de alerta avançadas, que são alertas orientados por fonte de dados, você pode usar a filtragem de escopo de múltiplas condições.

Esse recurso ajuda a reduzir alertas excessivos que podem levar à diminuição da capacidade de resposta ou eficácia na resolução de problemas importantes. Essa política ajuda a medir a eficácia das políticas de alerta e o engajamento dos administradores.

Você pode criar uma política de alerta avançada na seção **Alertas** > **Política de alerta avançada** > **Criar Política**. Você pode selecionar uma das seguintes Fontes de dados:

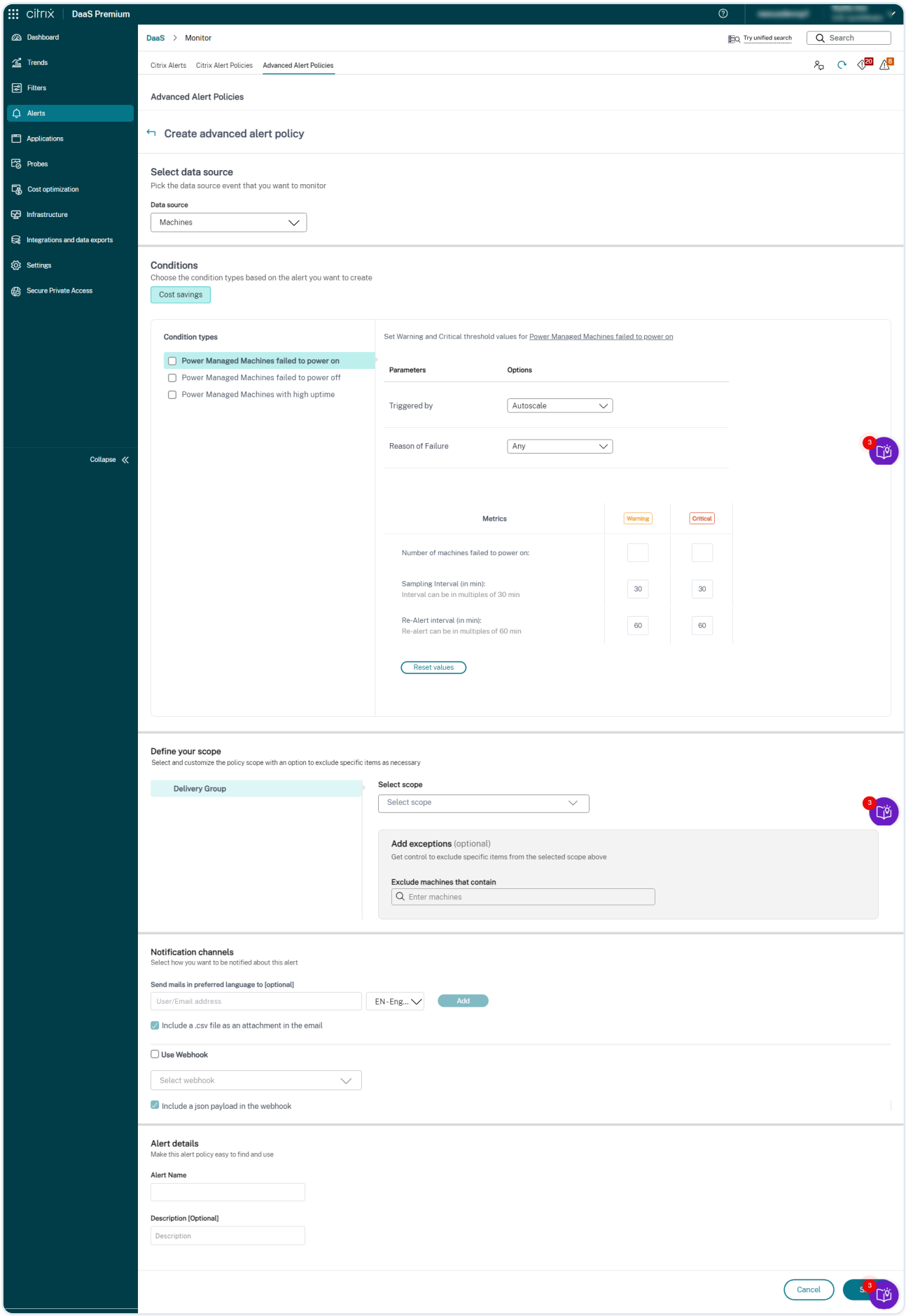
- Máquinas
- Serviço de Provisionamento
- StoreFront™

Alertas para economia de custos

Você pode criar alertas para economia de custos, o que ajuda a otimizar os custos. Atualmente, você pode criar alertas para máquinas.

Para criar alertas em Máquinas, faça o seguinte:

1. Clique na guia **Alertas** > **Políticas de Alerta Avançadas**. A página **Políticas de Alerta Avançadas** é exibida.
2. Clique em **Criar Política**. A seção **Criar Políticas de Alerta Avançadas** é exibida.
3. Selecione **Máquinas** na lista suspensa Fonte de dados. A condição de Economia de custos e os tipos de condição correspondentes são exibidos.



1. Selecione os seguintes tipos de condição conforme necessário:

- **Máquinas com gerenciamento de energia falharam ao ligar**
- **Máquinas com gerenciamento de energia falharam ao desligar**
- **Máquinas com gerenciamento de energia com alto tempo de atividade**

2. Selecione os parâmetros específicos e as opções correspondentes para cada uma das condições selecionadas.
3. Defina as métricas de Aviso e Crítico para o tipo de condição selecionado:
    - Para **Máquinas com gerenciamento de energia com alto tempo de atividade**:
        - Número de máquinas que excedem o limite de tempo de atividade
        - Intervalo de re-alerta (em min) o intervalo pode ser de no mínimo 60 min
    - Para **Máquinas com gerenciamento de energia falharam ao ligar** e **Máquinas com gerenciamento de energia falharam ao desligar**:
        - Número de máquinas que excedem o limite de tempo de atividade
        - Intervalo de amostragem (em min) os intervalos podem ser múltiplos de 30 min
        - Intervalo de re-alerta (em min) o re-alerta pode ser múltiplos de 60 min
4. Agende intervalos de re-alerta para os alertas selecionados conforme necessário.
5. Defina o escopo do alerta.
6. Defina os canais de notificação. Isso pode ser e-mail ou Webhook.
    - Você pode selecionar as seguintes caixas de seleção:
        - **Incluir um payload JSON como anexo no webhook**
        - **Incluir um arquivo CSV como anexo no e-mail**
7. Insira os **Detalhes do alerta**, como **Nome do alerta** e **Descrição** (opcional).
8. Clique em **Salvar**. O alerta é criado.

Alertas para Latência de Conexão SPA

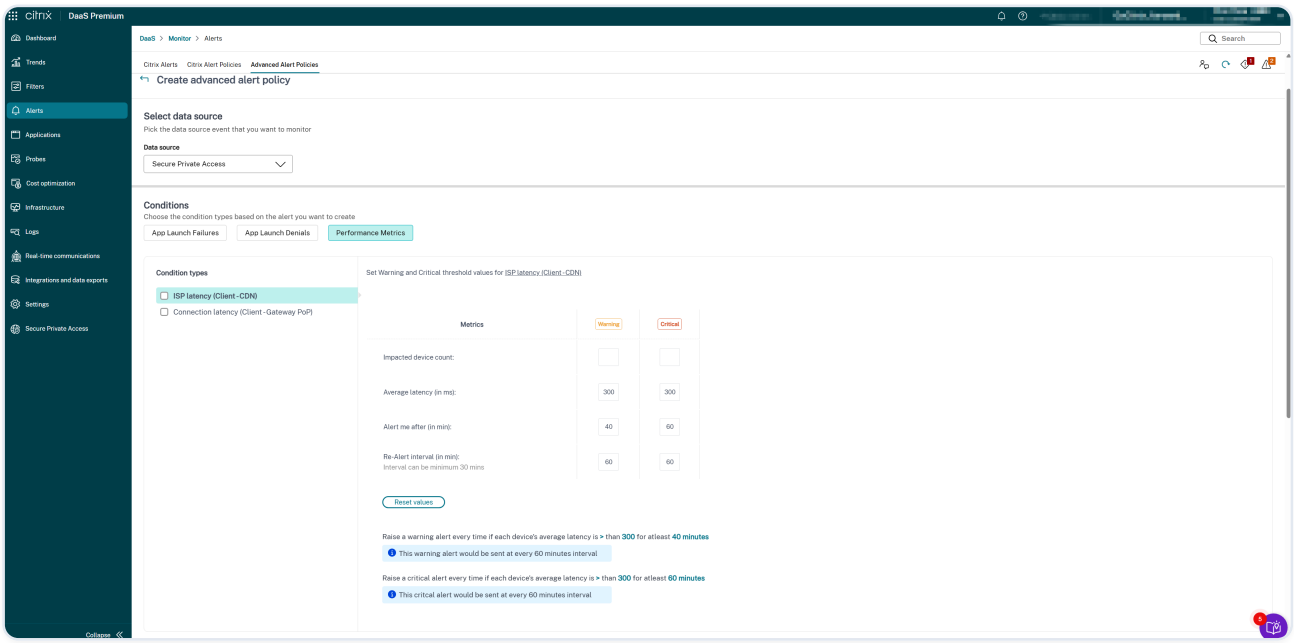
A estrutura de Políticas de Alerta Avançadas oferece suporte a alertas proativos para conectividade de Acesso Privado Seguro (SPA). Use esta política para detectar e agir sobre a latência de ponta a ponta que afeta as conexões de usuário do SPA.

CONFIGURAR ALERTA DE LATÊNCIA DE CONEXÃO SPA

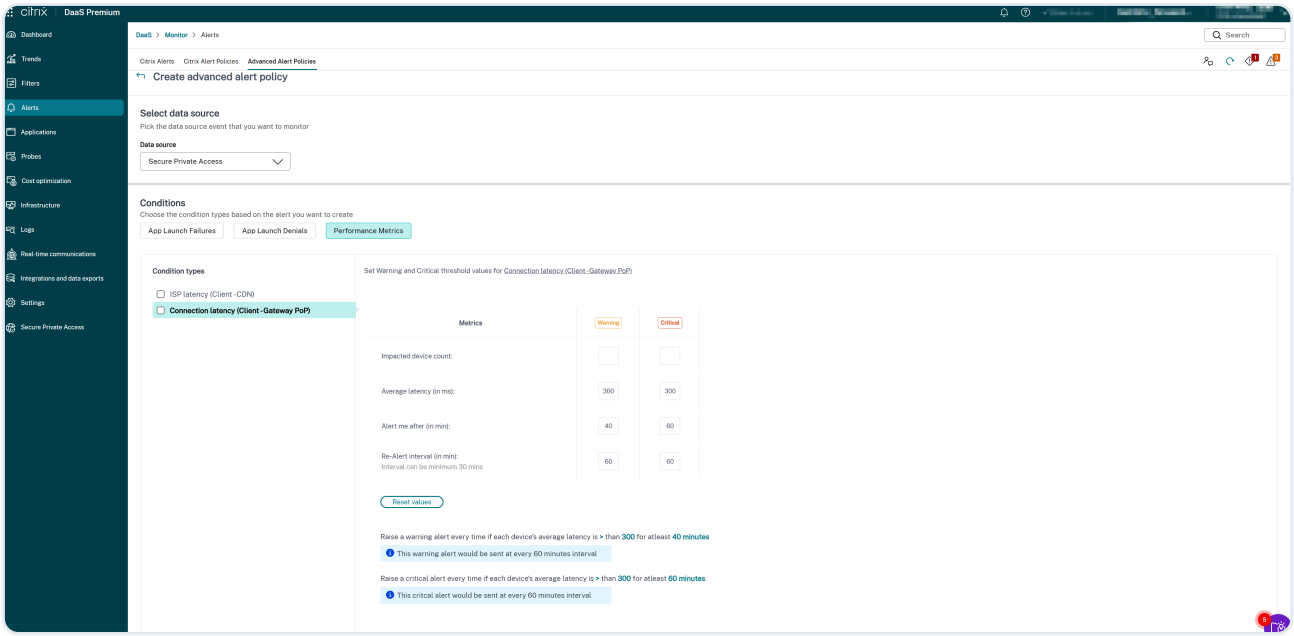
Para criar alertas para Latência de Conexão SPA, faça o seguinte:

1. Clique na guia **Alertas** > **Políticas de Alerta Avançadas**. A página **Políticas de Alerta Avançadas** é exibida.
2. Clique em **Criar Política**. A seção **Criar Políticas de Alerta Avançadas** é exibida.
3. Selecione **Acesso Privado Seguro** na lista suspensa Fonte de dados. A condição Latência de Conexão SPA é exibida.
4. Selecione os seguintes tipos de métrica conforme necessário:
    - **Latência do ISP (Cliente → CDN)**
    - **Latência de conexão (Cliente → PoP do Gateway)**

- Latência do ISP (Cliente → CDN)



- Latência de conexão (Cliente → PoP do Gateway)



1. Selecione os parâmetros específicos e as opções correspondentes para cada uma das métricas selecionadas.
2. Defina as métricas de Aviso e Crítico para o tipo de condição selecionado:
    - **Limite de latência (em ms)**: Defina os valores de Aviso (por exemplo, 150–200 ms) e Crítico (por exemplo, 300–400 ms)
    - **Usuários impactados (contagem)**: Número de usuários com latência acima do limite
    - **Intervalo de amostragem (em min)**: Com que frequência avaliar a latência (por exemplo, 5–15 minutos)
    - **Intervalo de re-alerta (em min)**: Mínimo de 60 minutos recomendado para evitar fadiga de alerta
3. Agende intervalos de re-alerta para os alertas selecionados conforme necessário.
4. Defina o escopo do alerta. Selecione site, grupo de entrega ou subconjunto direcionado.
5. Defina os canais de notificação. Isso pode ser e-mail ou Webhook.
    - Você pode selecionar as seguintes caixas de seleção:
        - **Incluir um payload JSON como anexo no webhook**
        - **Incluir um arquivo CSV como anexo no e-mail**
6. Insira os **detalhes do alerta**, como **Nome do Alerta** (por exemplo, "Latência de Conexão SPA – PoP Leste") e **Descrição** (opcional).
7. Clique em **Salvar**. O alerta é criado.

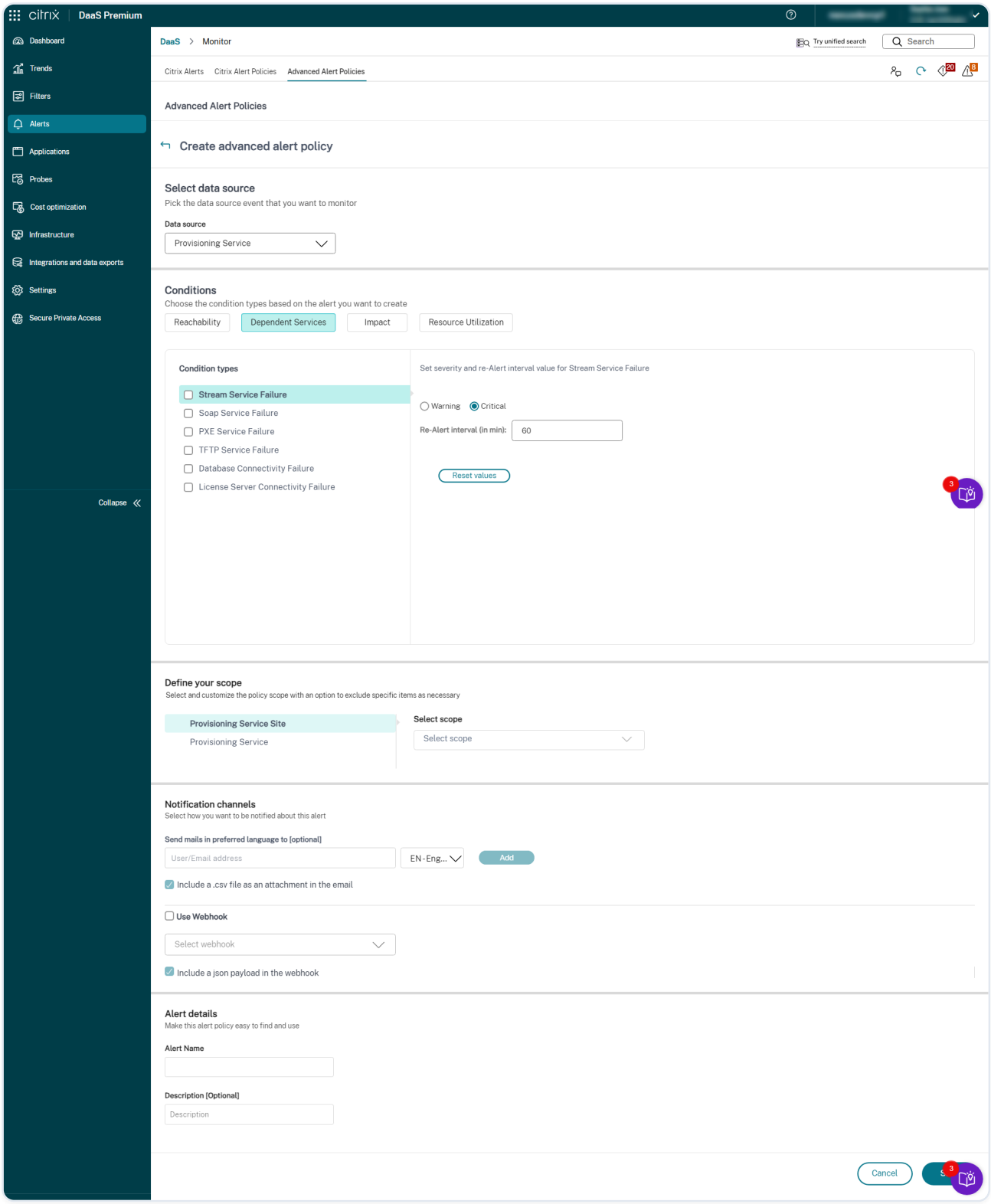
> Recomendação:

> Para alertas proativos, ajuste os limites de latência com base nas medições de linha de base por região. Inclua a integração de webhook para encaminhar alertas de alta latência para o gerenciamento de incidentes para uma triagem mais rápida.

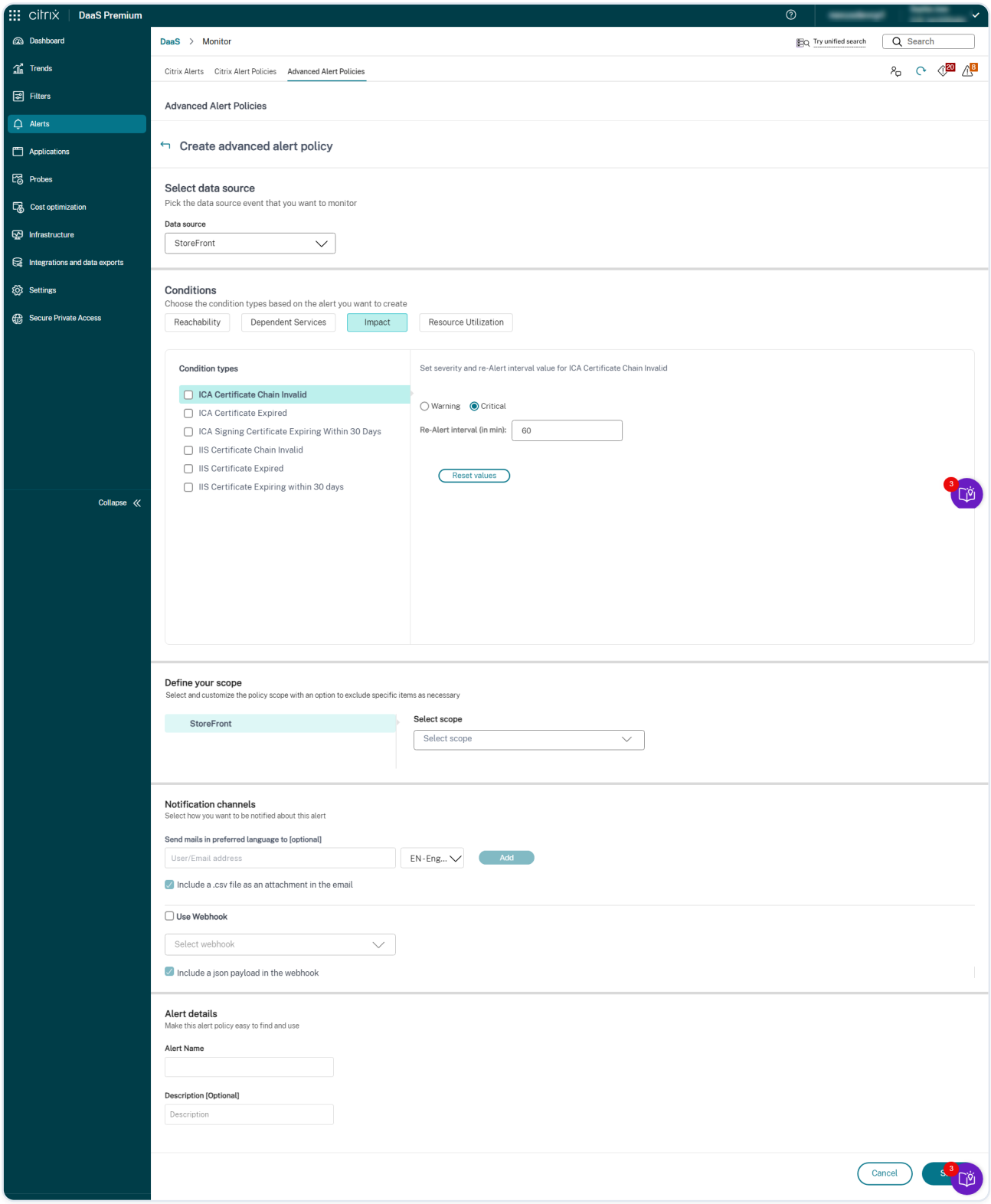
Políticas de infraestrutura

Você pode criar alertas para monitorar a integridade dos seguintes componentes do Citrix DaaS™ suportados:

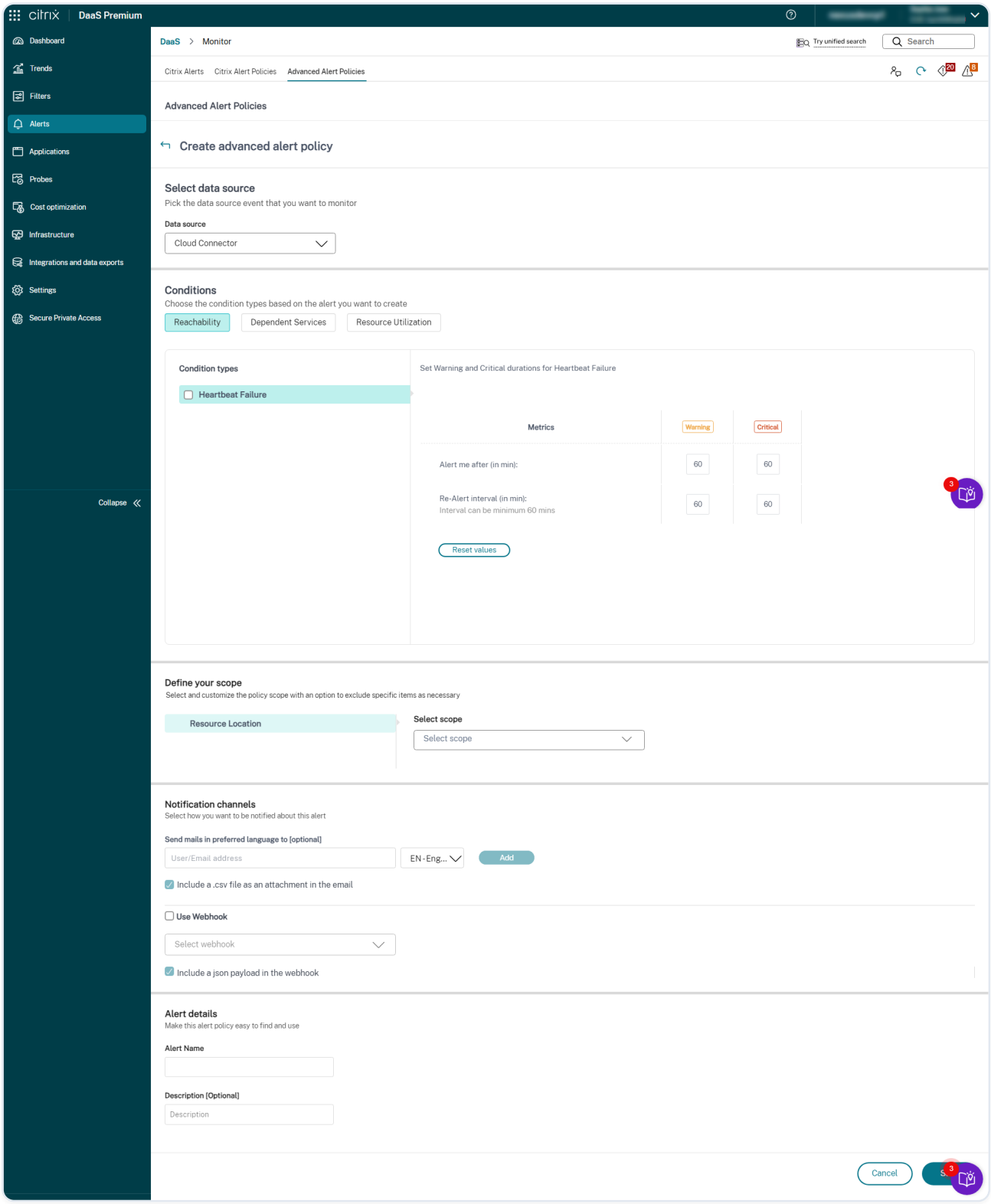
- Serviço de Provisionamento


citrix | DaaS Premium
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Secure Private Access
Collapse
DaaS > Monitor
Try unified search
Search
Citrix Alerts
Citrix Alert Policies
Advanced Alert Policies
Advanced Alert Policies
Create advanced alert policy
Select data source
Pick the data source event that you want to monitor
Data source
Provisioning Service
Conditions
Choose the condition types based on the alert you want to create
Reachability
Dependent Services
Impact
Resource Utilization
Condition types
Stream Service Failure
Soap Service Failure
PXE Service Failure
TFTP Service Failure
Database Connectivity Failure
License Server Connectivity Failure
Set severity and re-Alert interval value for Stream Service Failure
Warning
Critical
Re-Alert interval (in min):
60
Reset values
Define your scope
Select and customize the policy scope with an option to exclude specific items as necessary
Provisioning Service Site
Provisioning Service
Select scope
Select scope
Notification channels
Select how you want to be notified about this alert
Send mails in preferred language to [optional]
User/Email address
EN - Eng...
Add
Include a .csv file as an attachment in the email
Use Webhook
Select webhook
Include a json payload in the webhook
Alert details
Make this alert policy easy to find and use
Alert Name
Description [Optional]
Description
Cancel

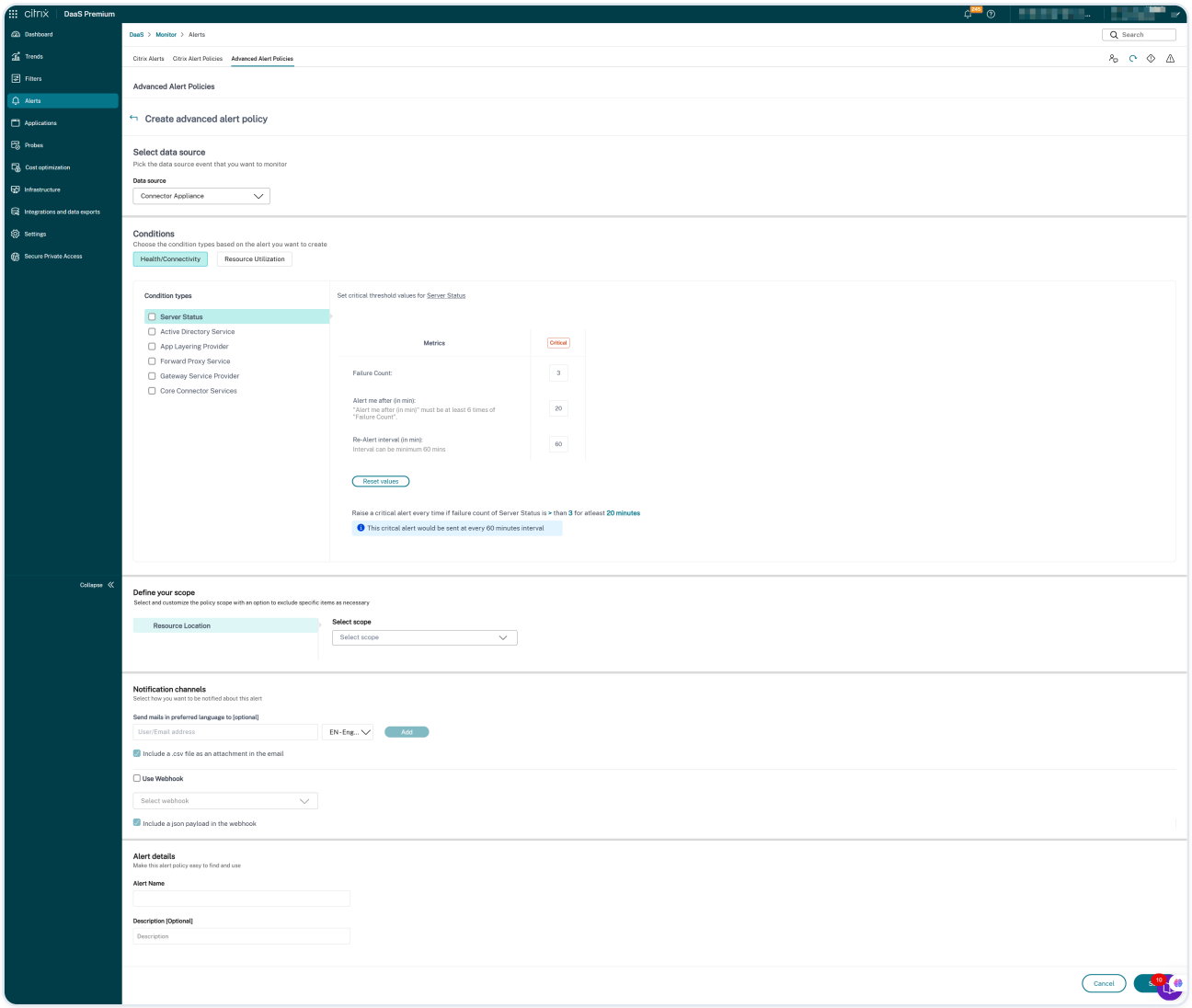
- StoreFront



- Cloud Connector



- Connector Appliance



Uma vez que a configuração do monitoramento de infraestrutura esteja concluída, você pode usar os dados de saúde disponíveis no Monitor para configurar alertas para qualquer componente necessário. Os administradores podem definir condições, escopos e meios de notificação para receber alertas importantes por e-mail ou um payload JSON por meio de webhooks. Os alertas gerados também estão disponíveis na seção **Alertas Citrix** para análise e gerenciamento.

Como parte da política de infraestrutura recém-introduzida, as condições de alerta são categorizadas em quatro seções, conforme a seguir:

- Acessibilidade
- Serviços dependentes
- Impacto
- Utilização de recursos

As condições dentro de cada categoria podem ser definidas com a severidade de **Crítico** e **Aviso** com base nas prioridades da sua organização. Você também pode agendar intervalos de re-alerta para esses alertas.

Você pode criar uma política de infraestrutura na seção **Alertas** > **Políticas de Alerta Citrix**. Você pode selecionar a categoria necessária e, em seguida, selecionar as condições necessárias para a política. Para obter mais informações sobre como criar uma política, consulte Criar políticas de alerta. Depois que a política é criada, você pode editar, excluir ou desabilitar a política na página Alertas Citrix.

Para obter mais detalhes sobre as condições suportadas em cada categoria e componente, consulte o seguinte:

- Métricas de saúde de provisionamento
- Métricas de saúde do StoreFront
- Métricas de saúde do Cloud Connector
- Métricas de saúde do Dispositivo Conector

Os seguintes dados são recebidos como um alerta por e-mail ou na página de Alertas Citrix:

CAMPO	DESCRIÇÃO
ID do Cliente	O ID do cliente do site.
Nível de alerta	Os valores possíveis são Crítico e Aviso.
Alvo	O nome da máquina para a qual o alerta é acionado.
Hora	A hora em que o alerta é acionado.
Escopo	O escopo da política.
Política	O nome da política.
Descrição	A descrição do problema para o qual o alerta é acionado.

Definir o escopo da política

Você pode definir o escopo do seu alerta e adicionar exceções. O alerta é gerado apenas para o escopo selecionado e o subescopo excluído usando adicionar exceções não é incluído na geração do alerta. Este recurso ajuda você a criar alertas em um nível granular.

Você pode criar notificações por e-mail ou por URLs de webhook. Você também pode selecionar seu idioma preferido no qual gostaria de receber alertas. Você também pode selecionar uma opção para receber os parâmetros do alerta em um anexo de arquivo .CSV para e-mail ou em um payload JSON por meio de uma URL de webhook. O anexo inclui detalhes dos parâmetros necessários. Para obter mais informações, consulte Aprimoramentos no conteúdo do alerta.

Os seguintes dados são recebidos como um alerta por e-mail ou na página **Citrix Alerts**:

CAMPO	DESCRIÇÃO
ID do Cliente	O ID do cliente do site.
Nível do alerta	Este valor é o valor predefinido para cada condição de alerta. Os valores possíveis são Crítico e Aviso.
Condição	Este valor é a condição definida ao criar a política. Por exemplo, o número de máquinas não registradas é igual ou superior a 20.
Alvo	O nome do grupo de entrega ou site para o qual o alerta é acionado.
Site	O nome do site.
Escopo	O escopo da política. Este valor também inclui o subescopo.
Política	O nome da política.
Descrição	A descrição do problema para o qual o alerta é acionado.

Como criar uma política de alerta avançada usando um script PowerShell?

Script PowerShell para criar uma política de alerta:

```
asnp Citrix.Monitor.*

# Add Parameters

$timeSpan = New-TimeSpan -Seconds 30
```

```
$alertThreshold = 1

$alarmThreshold = 2

# Add Target UID's

$targetIds = @()

$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"

# Add email addresses

$emailaddress = @()

$emailaddress += "loki@abc.com"

# Create new policy

$policy = New-MonitorNotificationPolicy -Name
"FailedMachinePercentageAlertCreationViaPowershell" -Description "Policy
created to test urm" -Enabled $true
```

SUBSTITUA A SEGUINTE LINHA PELA CONDIÇÃO CORRETA PARA FAILEDMACHINEPERCENTAGE

```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
FailedMachinePercentage -AlertThreshold $alertThreshold -AlarmThreshold
$alarmThreshold -AlertRenotification $timeSpan -AlarmRenotification
$timeSpan

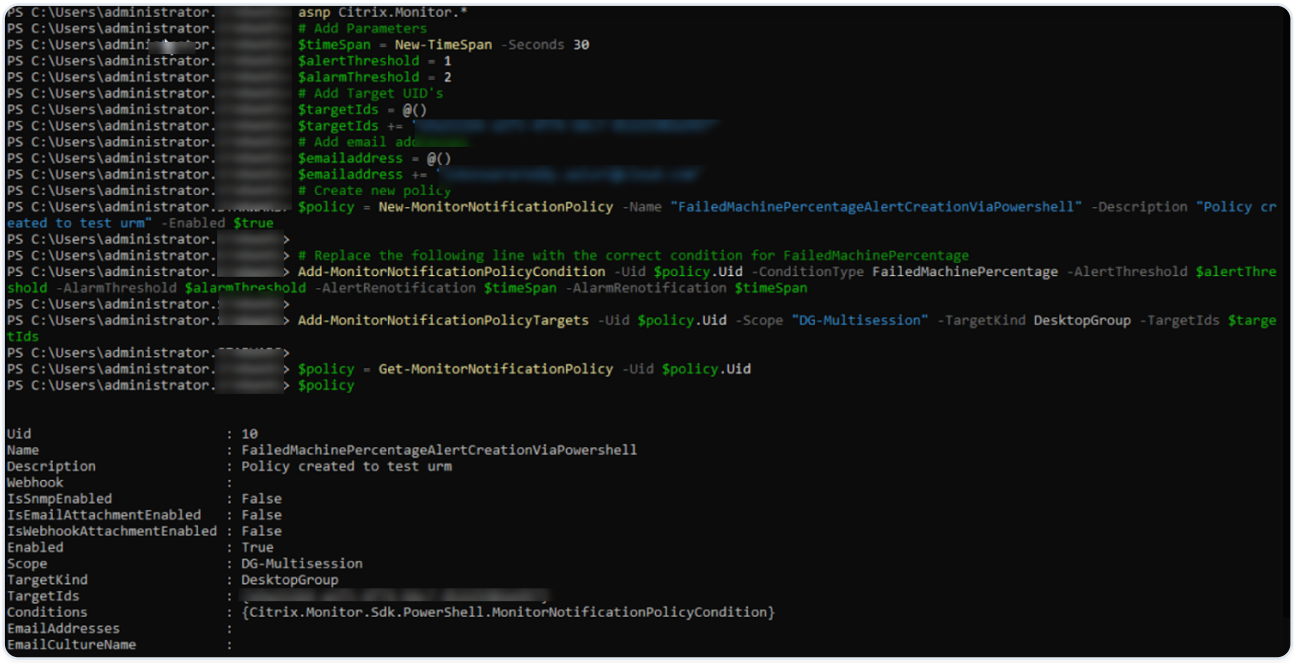


Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
Multisession" -TargetKind DesktopGroup -TargetIds $targetIds



$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid

$policy
```



Na imagem anterior, você pode ver que a política foi criada e o Uid é 10.

PARA ADICIONAR E-MAIL À CONFIGURAÇÃO

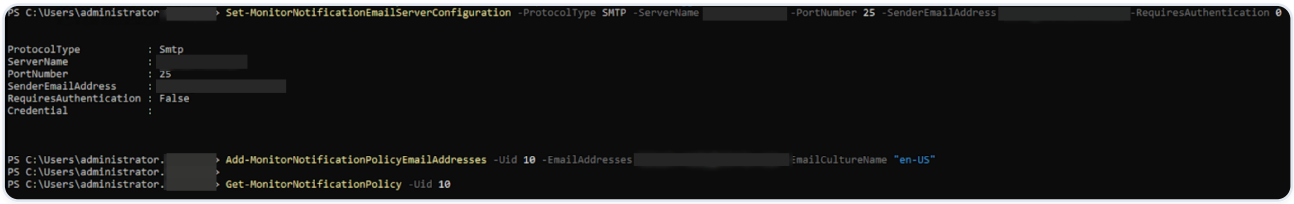
```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP
-ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80
-SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

PARA ADICIONAR E-MAIL À POLÍTICA

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid
-EmailAddresses $emailaddress -EmailCultureName "en-US"
```

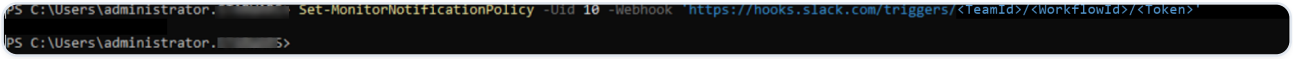
Script de exemplo para adicionar e-mail:

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
$emailaddress -EmailCultureName "en-US"
```



PARA ADICIONAR URL DE WEBHOOK À POLÍTICA

```
Set-MonitorNotificationPolicy –Uid $polcy.Uid –Webhook 'URL'
```

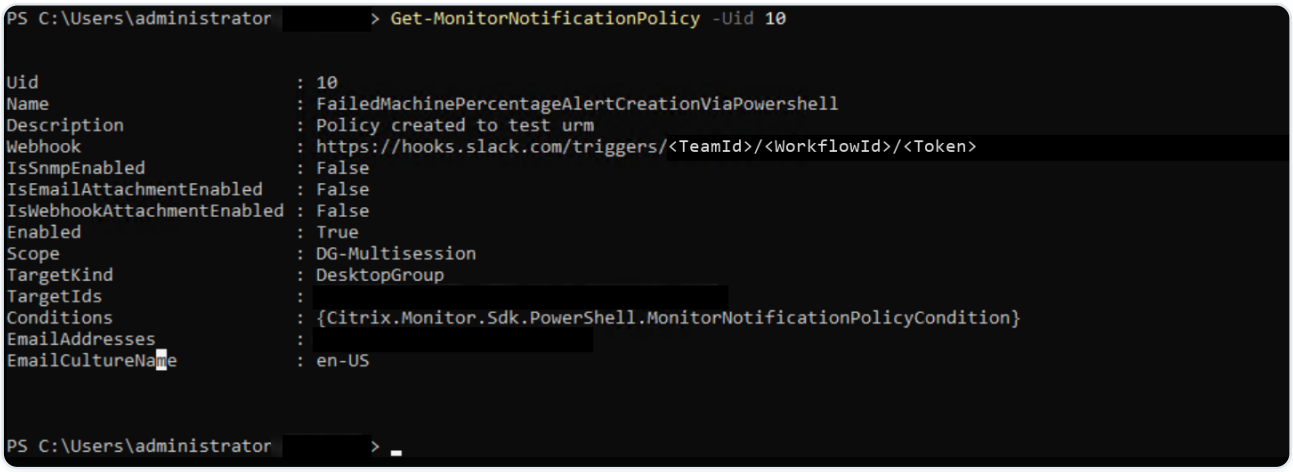


Script de exemplo para adicionar URL de webhook:

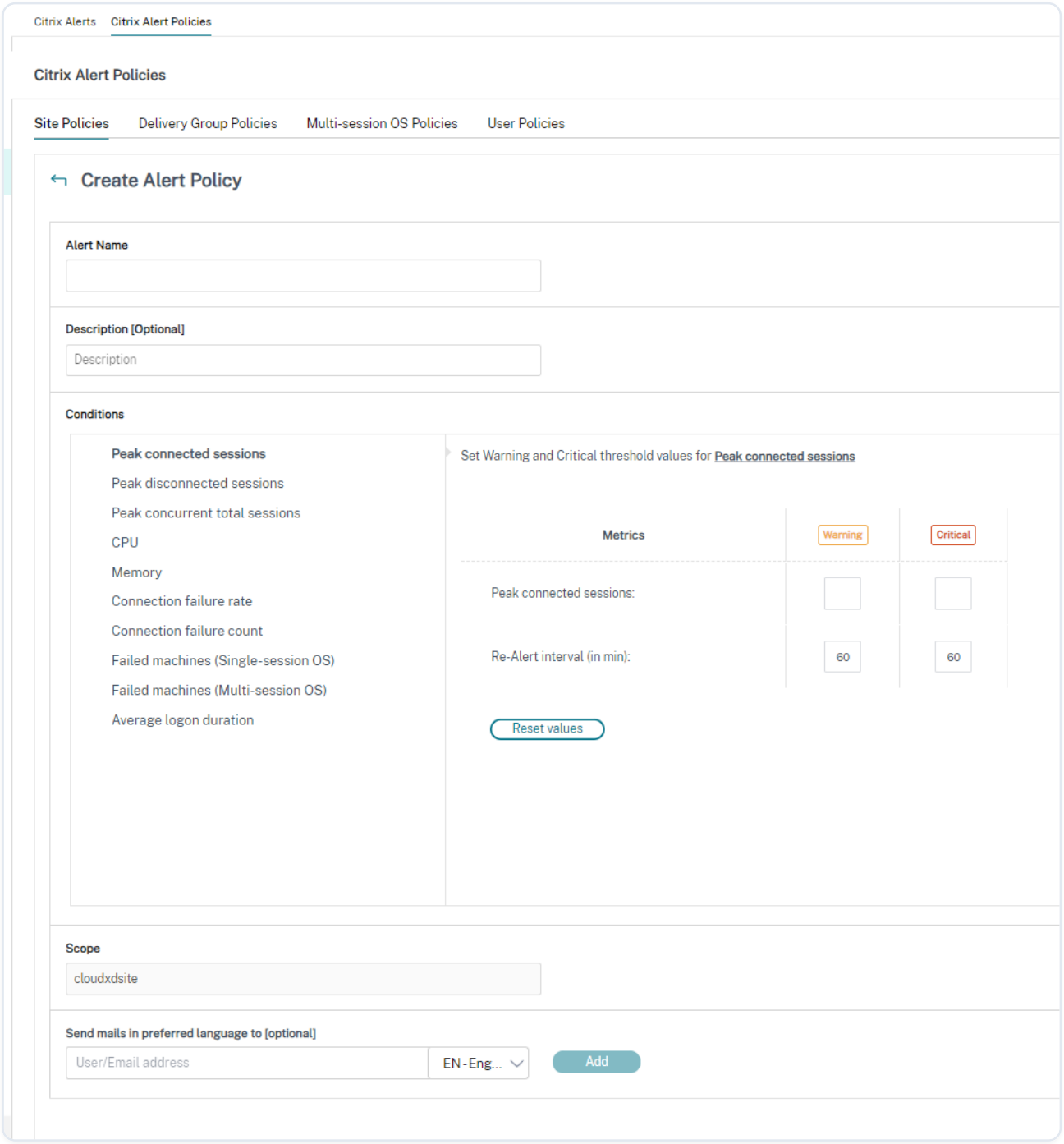
```
Set-MonitorNotificationPolicy –Uid 10  –Webhook  'https://hooks.slack.com/triggers/<TeamId>/<WorkflowId>/<Token>'
```

OBTER DETALHES DA POLÍTICA CRIADA

```
Get-MonitorNotificationPolicy -Uid 10
```



Criar políticas de alerta



Para criar uma política de alerta, por exemplo, para gerar um alerta quando um conjunto específico de critérios de contagem de sessões for atendido:

1. Vá para **Alertas** \> **Política de Alertas do Citrix** e selecione, por exemplo, Política de SO de Múltiplas Sessões.
2. Clique em **Criar**.
3. Nomeie e descreva a política, depois defina as condições que devem ser atendidas para que o alerta seja acionado. Por exemplo, especifique as contagens de Aviso e Crítico para Sessões Conectadas de Pico, Sessões Desconectadas de Pico e Sessões Totais Concorrentes de Pico.

Os valores de Aviso não devem ser maiores que os valores Críticos. Para obter mais informações, consulte Condições das políticas de alerta.

4. Defina o intervalo de Re-alerta. Se as condições para o alerta ainda forem atendidas, o alerta será acionado novamente neste intervalo de tempo e, se configurado na política de alerta, uma notificação por e-mail será gerada. Um alerta ignorado não gera uma notificação por e-mail no intervalo de re-alerta.
5. Defina o Escopo. Por exemplo, defina para um grupo de entrega específico.
6. Nas preferências de Notificação, especifique quem deve ser notificado por e-mail quando o alerta for acionado. As notificações por e-mail são enviadas via SendGrid. Certifique-se de que o endereço de e-mail `donotreplynotifications@citrix.com` esteja na lista de permissões da sua configuração de e-mail.
7. Clique em **Salvar**.

A criação de uma política com 20 ou mais grupos de entrega definidos no Escopo pode levar aproximadamente 30 segundos para concluir a configuração. Um spinner é exibido durante esse tempo.

A criação de mais de 50 políticas para até 20 grupos de entrega exclusivos (1000 destinos de grupo de entrega no total) pode resultar em um aumento no tempo de resposta (mais de 5 segundos).

Mover uma máquina contendo sessões ativas de um grupo de entrega para outro pode acionar alertas de grupo de entrega errôneos que são definidos usando parâmetros de máquina.

> **Nota:**
>
> Depois de excluir uma política de alerta, pode levar até 30 minutos para que as notificações de alerta geradas pela política parem.

Aprimoramentos no conteúdo do alerta

O recurso de alerta do Monitor foi aprimorado para incluir um anexo CSV e um payload JSON. Com esse aprimoramento, você pode obter detalhes do alerta em um anexo CSV por e-mail ou como um payload JSON se houver um webhook. Usando este anexo CSV ou payload JSON, você pode receber conteúdo enriquecido em um nível detalhado, auxiliando na rápida identificação e resolução de problemas.

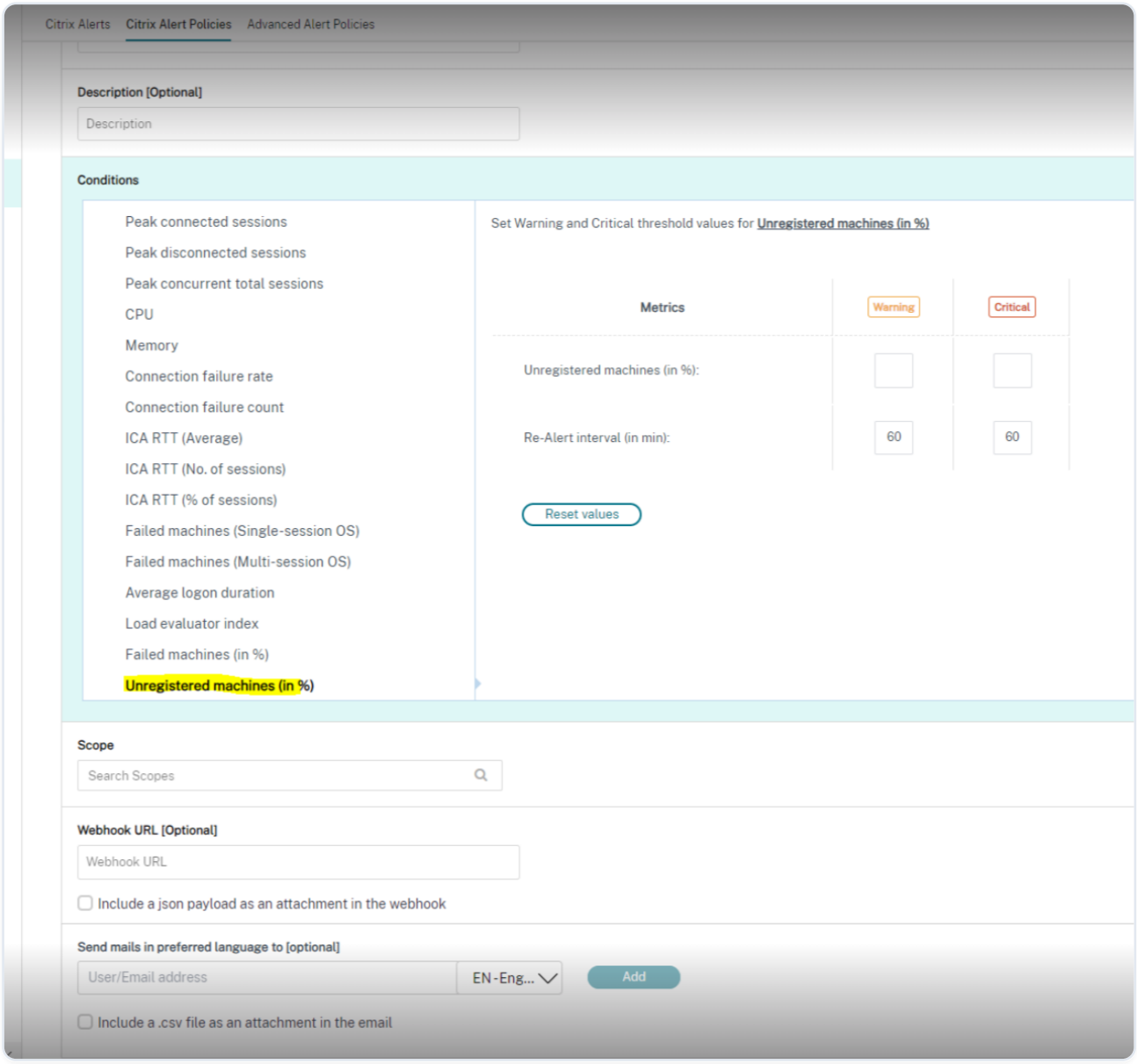
Atualmente, esse aprimoramento está disponível apenas nos seguintes alertas:

- Tempo de atividade da máquina
- Ações de inicialização com falha
- Ações de desligamento com falha
- Máquinas não registradas (%)

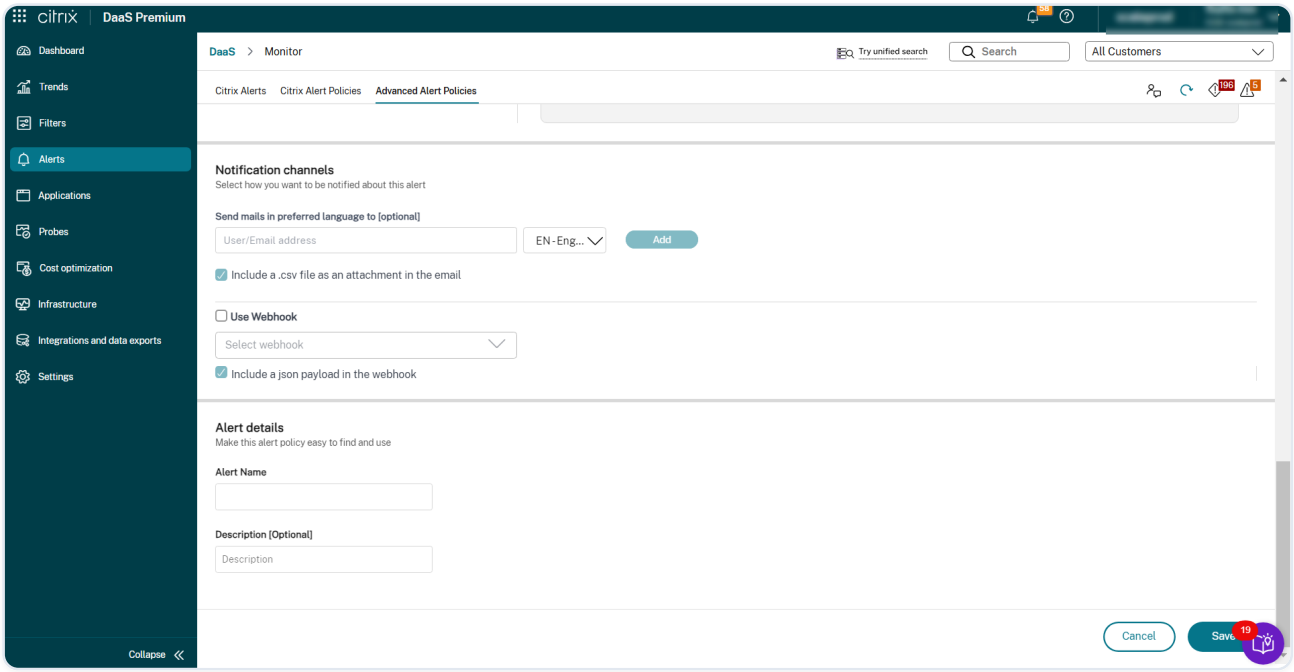
Para usar este recurso, navegar até o alerta e selecione as seguintes caixas de seleção:

- **Incluir um payload JSON como anexo no webhook**
- **Incluir um arquivo CSV como anexo no e-mail**

A seguir, uma captura de tela da seção **Políticas de Alerta do Citrix**:



Aqui está uma captura de tela da seção **Políticas de Alerta Avançadas**:



ANEXO CSV

A tabela a seguir fornece as colunas do anexo .CSV para todos os alertas suportados:

COLUNA	ALERTA APLICÁVEL
Nome da Máquina, Endereço IP e Nome do Grupo de Entrega	Tempo de atividade da máquina, Ação de desligamento falha e Ação de ligamento falha, e Máquinas não registradas (%)
Estado de Registro Atual, Data da Falha, Estado de Falha e Estado do Ciclo de Vida	Máquina não registrada (%)
Motivo da Falha da Última Ação de Energia, Última Ação de Energia Acionada Por, Tipo da Última Ação de Energia e Data de Conclusão da Última Ação de Energia	Ação de desligamento falha e Ação de inicialização falha
Estado de Energia, Data de Inicialização e Tempo Total de Atividade em Minutos	Tempo de atividade da máquina

PAYLOAD DO WEBHOOK

Alerta de Porcentagem de Máquinas Não Registradas

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
```

```
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Unregistered machines (in %)\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"CurrentRegistrationState\":\"Unregistered\",
\"FailureDate\":\"<Date of Failure>\",\"FaultState\":\"<Fault State of the
Machine>\",\"LifecycleState\":\"<Lifecycle state of the Machine>\"},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"CurrentRegistrationState\":\"Unregistered\",\"FailureDate\":\"<Date of
Failure>\",\"FaultState\":\"<Fault State of the Machine>\",
\"LifecycleState\":\"<Lifecycle state of the Machine>\"}]}"

}
```

Alerta de ações de inicialização falhas

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOn Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of the
DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"
```

```
}
```

Alerta de ações de desligamento falhas

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOff Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IPV4 Address of the Machine>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IPV4 Address of the Machine>\",\"DeliveryGroupName\":
\"<Name of the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"

}
```

Alerta de tempo de atividade da máquina

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Machine Uptime Alert\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
```

```
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"PowerState\":\"<On/Off>\",\"PoweredOnDate\":
\"2024-05-15T15:04:27.723\",\"TotalUptimeInMinutes\":180},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",\"PowerState\":
\"<ON/OFF>\",\"PoweredOnDate\":\"2024-05-15T15:04:27.723\",
\"TotalUptimeInMinutes\":\"<Uptime Duration>\"}]}"

}
```

Condições das políticas de alertas

Encontre abaixo as categorias de alerta, as ações recomendadas para mitigar o alerta e as condições de política integradas, se definidas. As políticas de alerta integradas são definidas para intervalos de alerta e realerta de 60 minutos.

Pico de Sessões Conectadas

- Verifique a exibição Tendências de Sessão do Monitor para picos de sessões conectadas.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário

Pico de Sessões Desconectadas

- Verifique a visualização Tendências de Sessão do Monitor para sessões desconectadas de pico.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.
- Faça logoff das sessões desconectadas, se necessário.

Pico de Sessões Totais Concorrentes

- Verifique a visualização Tendências de Sessão do Monitor em Monitor para sessões concorrentes de pico.
- Verifique se há capacidade suficiente para acomodar a carga da sessão.
- Adicione novas máquinas, se necessário.
- Faça logoff das sessões desconectadas, se necessário.

CPU

A porcentagem de uso da CPU indica o consumo geral da CPU no VDA, incluindo o dos processos. Você pode obter mais informações sobre a utilização da CPU por processos individuais na página **Detalhes da máquina** do VDA correspondente.

- Vá para **Detalhes da Máquina > Exibir Utilização Histórica > 10 Principais Processos**, identifique os processos que consomem a CPU. Certifique-se de que a política de monitoramento de processos esteja habilitada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.
- Encerre o processo, se necessário.
- Encerrar o processo faz com que os dados não salvos sejam perdidos.
- Se tudo estiver funcionando como esperado, adicione mais recursos de CPU no futuro.

> **Nota:**
>
> A configuração de política, **Habilitar monitoramento de recursos**, é permitida por padrão para o monitoramento de contadores de desempenho de CPU e memória em máquinas com VDAs. Se esta configuração de política estiver desabilitada, alertas com condições de CPU e memória não são acionados. Para obter mais informações, consulte Configurações de política de monitoramento.
>
> **Condições de política inteligente:**

  - **Escopo:** Grupo de entrega, escopo de SO multi-sessão
  - **Valores de limite:** Aviso - 80%, Crítico - 90%

Memória

A porcentagem de uso da memória indica o consumo geral de memória no VDA, incluindo o dos processos. Você pode obter mais informações sobre o uso da memória por processos individuais na página **Detalhes da máquina** do VDA correspondente.

- Vá para **Detalhes da Máquina > Exibir Utilização Histórica > 10 Principais Processos**, identifique os processos que consomem memória. Certifique-se de que a política de monitoramento de processos esteja habilitada para iniciar a coleta de estatísticas de uso de recursos em nível de processo.
- Encerre o processo, se necessário.

- Encerrar o processo causa a perda de dados não salvos.
- Se tudo estiver funcionando como esperado, adicione mais memória no futuro.

> **Nota:**
>
> A configuração de política **Habilitar monitoramento de recursos** é permitida por padrão para o monitoramento de contadores de desempenho de CPU e memória em máquinas com VDAs. Se esta configuração de política estiver desabilitada, alertas com condições de CPU e memória não são acionados. Para obter mais informações, consulte Configurações de política de monitoramento.
>
> **Condições de política inteligente:**
>
> - **Escopo:** Grupo de entrega, escopo de SO multi-sessão
> - **Valores de limite:** Aviso - 80%, Crítico - 90%

Taxa de Falha de Conexão

Porcentagem de falhas de conexão na última hora.

- Calculado com base no total de falhas em relação ao total de conexões tentadas.
- Verifique a visualização Tendências de Falhas de Conexão do Monitor para eventos registrados no log de Configuração.
- Determine se aplicativos ou desktops estão acessíveis.

Contagem de Falhas de Conexão

Número de falhas de conexão na última hora.

- Verifique a visualização Tendências de Falhas de Conexão do Monitor para eventos registrados no log de Configuração.
- Determine se aplicativos ou desktops estão acessíveis.

ICA® RTT (Média)

Tempo médio de ida e volta do ICA.

- Verifique o Citrix ADM para uma análise detalhada do RTT do ICA para determinar a causa raiz. Para obter mais informações, consulte a documentação do Citrix ADM.

- Se o Citrix ADM não estiver disponível, verifique a visualização Detalhes do Usuário do Monitor para o RTT do ICA e a Latência, e determine se é um problema de rede ou um problema com aplicativos ou desktops.

ICA RTT (Nº de Sessões)

Número de sessões que excedem o tempo de ida e volta ICA limite.

- Verifique o Citrix ADM para o número de sessões com alto RTT ICA. Para mais informações, consulte a documentação do Citrix ADM.
- Se o Citrix ADM não estiver disponível, entre em contato com a equipe de rede para determinar a causa raiz.

  Condições da política inteligente:

  - **Escopo:** Grupo de entrega, escopo de SO multissessão
  - **Valores limite:** Aviso - 300 ms para 5 ou mais sessões, Crítico - 400 ms para 10 ou mais sessões

RTT ICA (% de Sessões)

Porcentagem de sessões que excedem o tempo médio de ida e volta ICA.

- Verifique o Citrix ADM para o número de sessões com alto RTT ICA. Para mais informações, consulte a documentação do Citrix ADM.
- Se o Citrix ADM não estiver disponível, entre em contato com a equipe de rede para determinar a causa raiz.

RTT ICA (Usuário)

Tempo de ida e volta ICA que é aplicado às sessões iniciadas pelo usuário especificado. O alerta é acionado se o RTT ICA for maior que o limite em pelo menos uma sessão.

Máquinas com falha (SO de sessão única)

Número de máquinas de SO de sessão única com falha. As falhas podem ocorrer por várias razões, conforme mostrado nos painéis Monitor e Filtros.

- Execute os diagnósticos do Citrix Scout para determinar a causa raiz. Para mais informações, consulte Solucionar problemas do usuário.

  Condições de política inteligente:

  - **Escopo:** Escopo do grupo de entrega

- **Valores de limite:** Aviso - 1, Crítico - 2

Máquinas com falha (SO multiusuário)

Número de máquinas de SO multiusuário com falha. As falhas podem ocorrer por vários motivos, conforme mostrado nas visualizações do Painel de Monitoramento e Filtros.

- Execute os diagnósticos do Citrix Scout para determinar a causa raiz.

  Condições de política inteligente:

  - **Escopo:** Grupo de entrega, escopo de SO multiusuário
  - **Valores de limite:** Aviso - 1, Crítico - 2

Máquinas com falha (em %)

A porcentagem de máquinas de SO de sessão única e multiusuário com falha em um grupo de entrega, calculada com base no número de máquinas com falha. Essa condição de alerta permite configurar limites de alerta como uma porcentagem de máquinas com falha em um grupo de entrega e é calculada a cada 30 segundos. As falhas podem ocorrer por vários motivos, conforme mostrado nas visualizações do Painel de Monitoramento e Filtros. Execute os diagnósticos do Citrix Scout para determinar a causa raiz. Para obter mais informações, consulte Solucionar problemas do usuário.

Ação de ligar com falha e ação de desligar com falha

Número de ações de ligar com falha e número de ações de desligar com falha em um grupo de entrega, calculados com base no número de **Máquinas Gerenciadas por Energia** que falharam ao ligar ou desligar. Essa condição de alerta permite configurar limites de alerta como o número de **Máquinas Gerenciadas por Energia** que falharam ao ligar ou desligar em um grupo de entrega e é calculada a cada 30 minutos.

O administrador pode configurar os seguintes parâmetros para esses alertas na política de alerta avançada:

- Acionado por: O que acionou a ação de energia
- Motivo da falha: Por que a ação falhou
- Limite: Número limite de máquinas que falharam na ação de energia para acionar a política
- Intervalo de amostragem: O intervalo em que a ação de energia com falha deve ser verificada
- Intervalo de reenvio de alerta: Após quanto tempo o alerta deve ser reenviado

Falhas podem ocorrer por vários motivos, conforme mostrado nas exibições do Painel do Monitor e Filtros. Execute os diagnósticos do Citrix Scout para determinar a causa raiz. Para obter mais informações, consulte Solucionar problemas do usuário.

Máquinas não registradas (em %)

Uma máquina é considerada não registrada quando se torna instável devido a uma reinicialização ou quando há um problema de comunicação entre o delivery controller™ e as máquinas virtuais. A **Máquinas não registradas (em %)** é a porcentagem de máquinas OS de sessão única e multissessão não registradas em um grupo de entrega, calculada com base no número de máquinas não registradas. Esta condição de alerta permite configurar valores de limite de aviso e críticos como uma porcentagem de máquinas não registradas em um grupo de entrega. Você pode definir um intervalo para o reenvio do alerta. Você também pode adicionar um e-mail para receber uma notificação quando as condições forem atendidas para **Máquinas não registradas (em %)**. Quando o valor limite crítico ou de aviso é excedido, alertas e e-mails são gerados. Você pode visualizar alertas em **Alertas do Citrix**. Você pode filtrá-lo pela categoria **Máquinas não registradas (em %)** e para o estado e tempo necessários.

> **Nota:**
>
> O valor crítico deve ser maior que o valor de aviso.

> **Condições da política:**

- **Escopo**: OS de sessão única e grupo de entrega de OS multissessão
- **Valores limite**: Aviso e Crítico

Alerta de tempo de atividade da máquina

O tempo de atividade da máquina em um grupo de entrega é calculado com base no número de horas por dia, horas por semana ou horas por mês para uma máquina que está ligada em um grupo de entrega. Esta condição de alerta permite configurar limites de alerta como as horas em que uma máquina está ligada em um grupo de entrega. Os alertas de tempo de atividade da máquina funcionam da seguinte forma no caso de:

- Horas por dia - Você pode especificar o número de horas em que uma máquina fica ligada por dia e é calculado a cada 30 minutos. O número máximo de horas por dia que você pode definir é de 24 horas.

- Horas por semana - Você pode especificar o número de horas que uma máquina fica ligada por semana e é calculado a cada seis horas. O número máximo de horas por semana que você pode definir é de 168 horas.
- Horas por mês - Você pode especificar o número de horas que uma máquina fica ligada por mês e é calculado uma vez por dia. O número máximo de horas por mês é de 720 horas. O valor mínimo do intervalo de re-alerta que você pode definir é de 60 minutos. Você pode inserir o número de máquinas que excedem o valor limite de tempo de atividade da máquina na seção de alertas de Aviso e Crítico. Você também pode adicionar exceções para quaisquer máquinas.

Por exemplo, se houver cinco grupos de entrega adicionados para este alerta e se no primeiro grupo de entrega e no quarto grupo de entrega, o número de máquinas exceder os valores limite de aviso ou crítico, o alerta será acionado separadamente para o primeiro grupo de entrega e para o quarto grupo de entrega.

Este alerta ajuda os administradores a analisar o tempo de atividade das máquinas e, com base nessa análise, os administradores podem ajudar a otimizar o custo. Você também pode receber detalhes do alerta em um anexo CSV em um e-mail ou por meio de um payload JSON no caso de um webhook.

Duração Média do Logon

Duração média do logon para logons que ocorreram na última hora.

- Verifique o Painel do Monitor para obter métricas atualizadas sobre a duração do logon. Um grande número de usuários fazendo logon em um curto período de tempo pode aumentar a duração do logon.
- Verifique a linha de base e a análise dos logons para identificar a causa. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

  Condições da política inteligente:

  - **Escopo:** Grupo de entrega, escopo de SO multi-sessão
  - **Valores limite:** Aviso - 45 segundos, Crítico - 60 segundos

Duração do Logon (Usuário)

Duração do logon para logons do usuário especificado que ocorreram na última hora.

Índice do Avaliador de Carga

Valor do Índice do Avaliador de Carga nos últimos 5 minutos.

- Verifique o Monitor para Máquinas de SO de Multi-sessão que possam ter uma carga de pico (Carga máxima). Visualize tanto o Painel (falhas) quanto o relatório de Tendências do Índice do Avaliador de Carga.

  Condições de política inteligente:

  - **Escopo:** Grupo de entrega, escopo de SO de Multi-sessão
  - **Valores de limite:** Aviso - 80%, Crítico - 90%

Configurar políticas de alerta com webhooks

Além das notificações por e-mail, você pode configurar políticas de alerta com webhooks.

Nota: Este recurso requer a versão 7.11 ou posterior do(s) Delivery Controller(s).

Você pode configurar uma política de alerta com um callback HTTP ou um POST HTTP usando cmdlets do PowerShell. Eles foram estendidos para suportar webhooks.

Para obter informações sobre a criação de um novo fluxo de trabalho do Octoblu e a obtenção do URL de webhook correspondente, consulte o Octoblu Developer Hub.

Para configurar um URL de webhook para uma nova política de alerta ou para uma política existente, use os seguintes cmdlets do PowerShell.

Criar política de alerta com um URL de webhook:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description
<Policy description> -Enabled $true -Webhook <Webhook URL>
```

Adicionar um URL de webhook a uma política de alerta existente:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

Para obter ajuda sobre os comandos do **PowerShell**, use a ajuda do PowerShell, por exemplo:

```
Get-Help  <Set-MonitorNotificationPolicy>
```

As notificações geradas a partir da política de alerta acionam o webhook com uma chamada POST para o URL do webhook. A mensagem POST contém as informações da notificação em formato JSON:

```
{"NotificationId" : \<Notification Id\>,

"Target" : \<Notification Target Id\>,

"Condition" : \<Condition that was violated\>,

"Value" : \<Threshold value for the Condition\>,

"Timestamp": \<Time in UTC when notification was generated\>,

"PolicyName": \<Name of the Alert policy\>,

"Description": \<Description of the Alert policy\>,

"Scope" : \<Scope of the Alert policy\>,

"NotificationState": \<Notification state critical, warning, healthy or dismissed\>,

"Site" : \<Site name\>}
```

Configurar políticas de alerta com ServiceNow

Você pode configurar políticas de alerta para enviar notificações diretamente para o ServiceNow (SNOW), permitindo uma integração perfeita com seus fluxos de trabalho de Gerenciamento de Serviços de TI (ITSM). Essa integração permite que os alertas gerados no Citrix Monitor sejam automaticamente encaminhados para o ServiceNow para rastreamento centralizado, escalonamento e resolução de incidentes.

BENEFÍCIOS DA INTEGRAÇÃO COM O SERVICENOW

- **Gerenciamento unificado de alertas**: Crie, atualize e gerencie incidentes do ServiceNow diretamente na interface do Citrix Monitor sem alternar entre os sistemas.
- **Configuração automática de ITSM**: O Monitor recupera automaticamente a configuração necessária do ServiceNow, como URLs de webhook, reduzindo a complexidade da configuração manual.
- **Resposta simplificada a incidentes**: Os alertas são encaminhados para o ServiceNow para rastreamento e resolução centralizados de incidentes, melhorando a eficiência operacional.

PRÉ-REQUISITOS

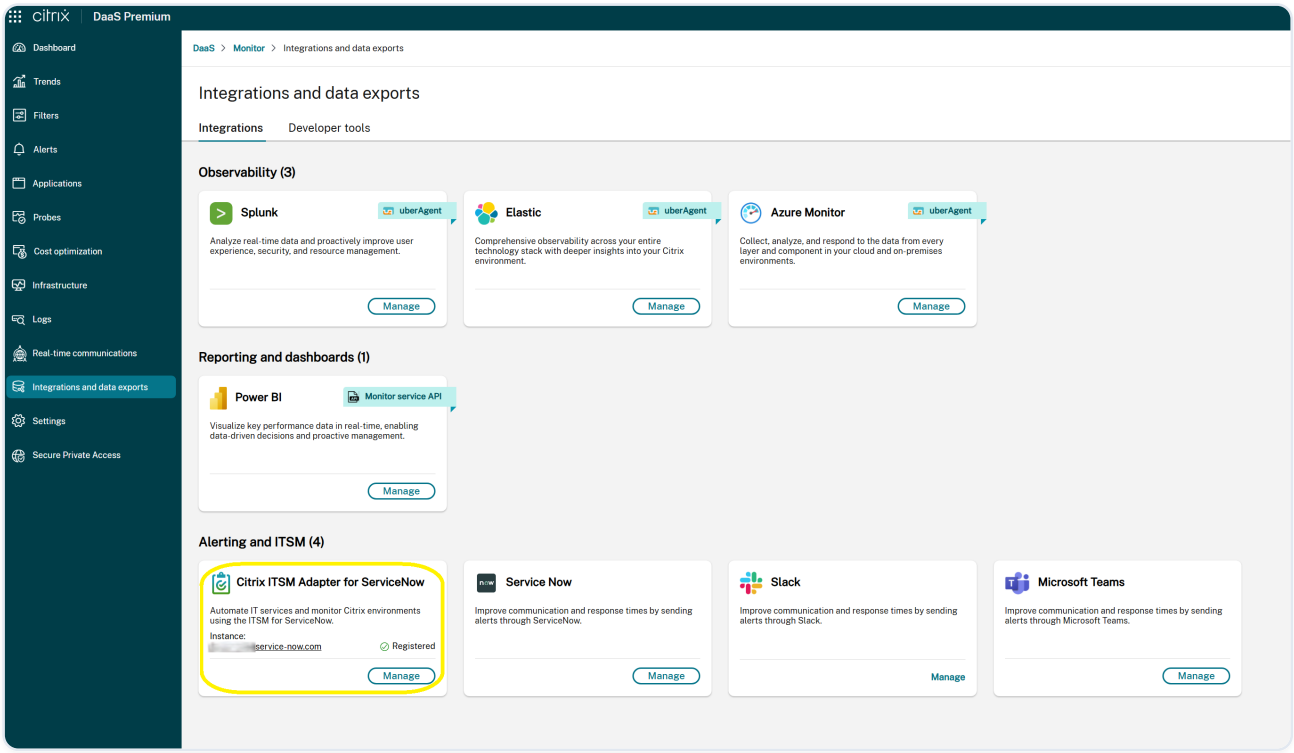
Antes de configurar a integração com o ServiceNow, certifique-se do seguinte:

- Uma instância do ServiceNow está configurada no serviço ITSM Adapter.
- Você tem as permissões necessárias para gerenciar políticas de alerta no Monitor.

VERIFICAR O STATUS DA INTEGRAÇÃO COM O SERVICENOW

Você pode visualizar o status da integração com o serviço ITSM Adapter na página **Monitor** > **Integrações e Exportações de Dados**. Esta página exibe:

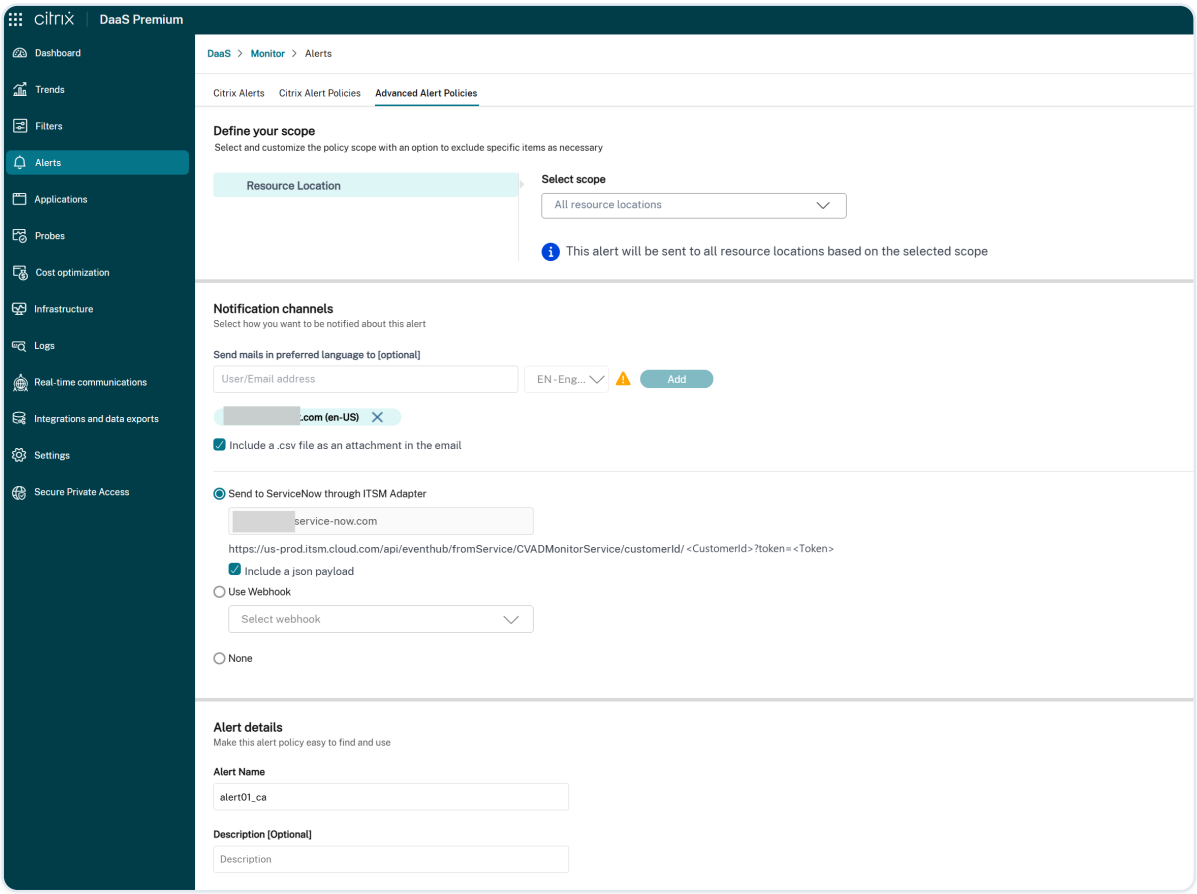
- O status atual da integração:
  - **Começar**: Indica que a integração do ITSM Adapter não foi configurada. Selecione esta opção para iniciar o processo de configuração inicial.
  - **Gerenciar**: Indica que a integração do ITSM Adapter está ativa e operacional. Selecione esta opção para visualizar ou modificar suas configurações de integração com o ServiceNow.
- A URL da instância do ServiceNow associada (visível apenas quando uma instância do ServiceNow foi configurada no ITSM Adapter).



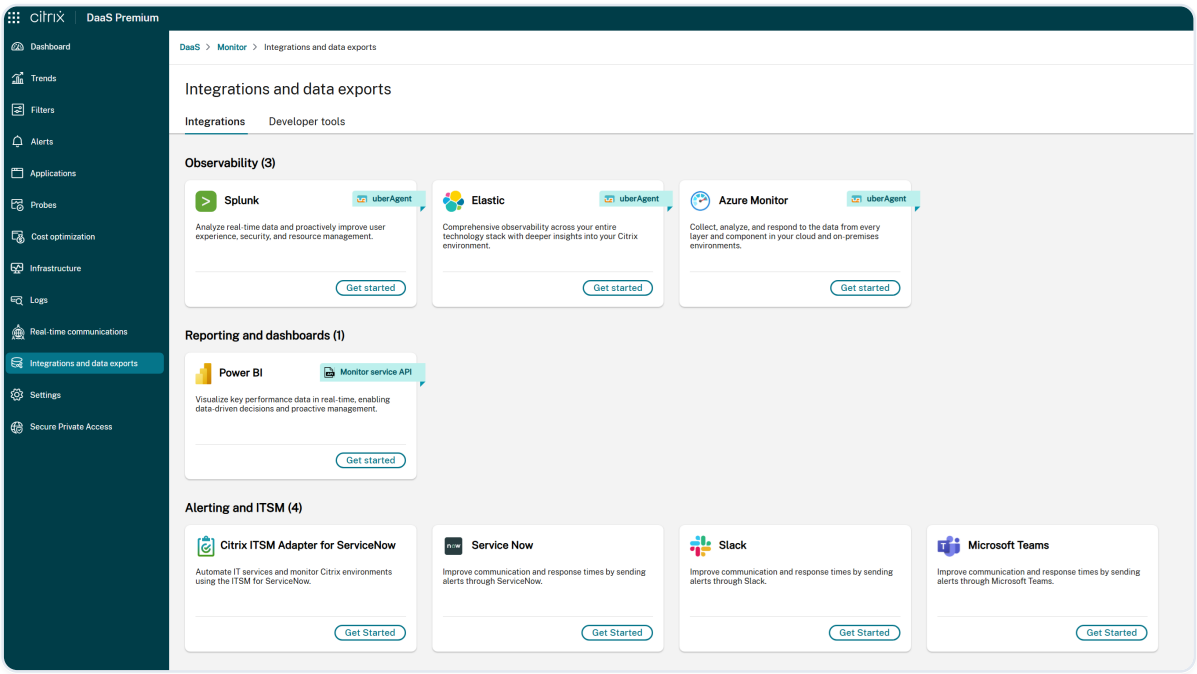
CONFIGURAR UMA POLÍTICA DE ALERTA COM NOTIFICAÇÕES DO SERVICENOW

Para configurar uma política de alerta para enviar notificações ao ServiceNow:

1. Vá para **Alertas** > **Política de Alertas do Citrix** e selecione a categoria da política (por exemplo, Política de SO Multissessão).
2. Clique em **Criar** para criar uma nova política ou selecione uma política existente e clique em **Editar**.
3. Configure as condições da política conforme necessário.
4. Na seção **Preferências de notificação**, procure a opção **Integração do ServiceNow**:
    - **Se o Adaptador ITSM estiver disponível:**
        - Marque a caixa de seleção para habilitar as notificações de alerta via ServiceNow para esta política.
        - A URL da instância do ServiceNow associada é exibida para referência.
        - Se a política já tiver um webhook configurado, uma mensagem de aviso informará que a habilitação da integração do ServiceNow substitui a configuração de webhook existente.



- **Se o Adaptador ITSM não estiver disponível:**
  - Uma mensagem indica que a integração ITSM não está configurada no momento.
  - Clique em **Começar** para acessar a configuração da integração. Para obter detalhes, consulte a documentação.



5. Clique em **Salvar** para salvar a política.

Uma vez configurados, os alertas que atendem às condições da política são automaticamente encaminhados para o ServiceNow, onde podem ser gerenciados como incidentes ou eventos com base na sua configuração ITSM.

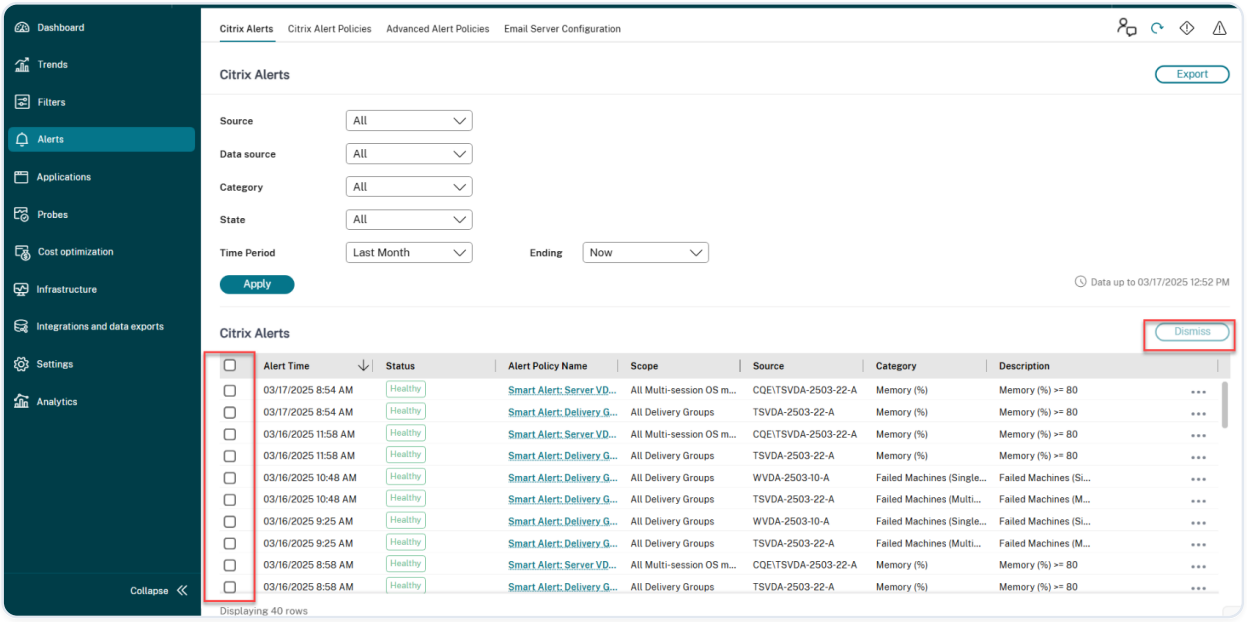
Descarte em massa de alertas

Este recurso otimiza o processo de gerenciamento de alertas para administradores, proporcionando flexibilidade e reduzindo a fadiga de alertas. Os administradores podem descartar alertas em massa com base no tempo, tipo ou categoria, simplificando o gerenciamento de alertas durante a manutenção ou ao lidar com hipervisores e outros ambientes.

O descarte em massa de alertas ajuda os administradores a gerenciar sua carga de trabalho de forma eficiente e os impede de serem sobrecarregados por um alto volume de alertas.

Etapas para descartar alertas em massa

1. navegar para a guia **Alertas** > **Alertas Citrix**. Os alertas são exibidos.



2. Selecione uma opção em **Origem**, **Categoria**, **Estado** ou **Período de Tempo** para filtrar os alertas que você deseja descartar. Os alertas específicos são exibidos.
3. Selecione a caixa de seleção ao lado de um alerta específico ou na parte superior para selecionar todos os alertas.
4. Clique em **Descartar**. Uma notificação aparece para confirmar o descarte dos alertas.
5. Clique em **Sim**. Os alertas selecionados são marcados como *descartados*, e o status do alerta é atualizado de acordo.

Configuração de webhook usando o SDK do PowerShell

O recurso de configuração de webhook usando o SDK do PowerShell permite que os administradores criem, modifiquem, excluam e listem perfis de webhook. Este recurso oferece flexibilidade na configuração de webhooks, permitindo a especificação de cabeçalhos, tipos de autenticação, tipos de conteúdo, payloads e URLs de webhook.

> **Nota:**
>
> O formato de payload suportado é texto e o usuário final deve habilitar o texto em seu webhook.

> O formato de payload mais recente é:

```
{"text": "This is a message from a Webex incoming webhook."}
```

Criar um webhook

Você pode usar o seguinte comando PowerShell de exemplo para criar um perfil de webhook:

Criar um webhook sem cabeçalho de autorização:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"


Add-MonitorWebhookProfile -Name "webhookprofile1" -Description
```

```
"Description" -Url $url -Headers $headers -PayloadFormat $payloads
-Platform Slack -Type Webhook -MethodType POST
```

Criar um webhook com cabeçalho de autorização:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$headers.Add("Authorization", "Basic <Fill this field with the
authorization token>")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"


Add-MonitorWebhookProfile -Name "webhookprofile1" -Description
"Description" -Url $url -Headers $headers -PayloadFormat $payloads
-Platform Slack -Type Webhook -MethodType POST
```

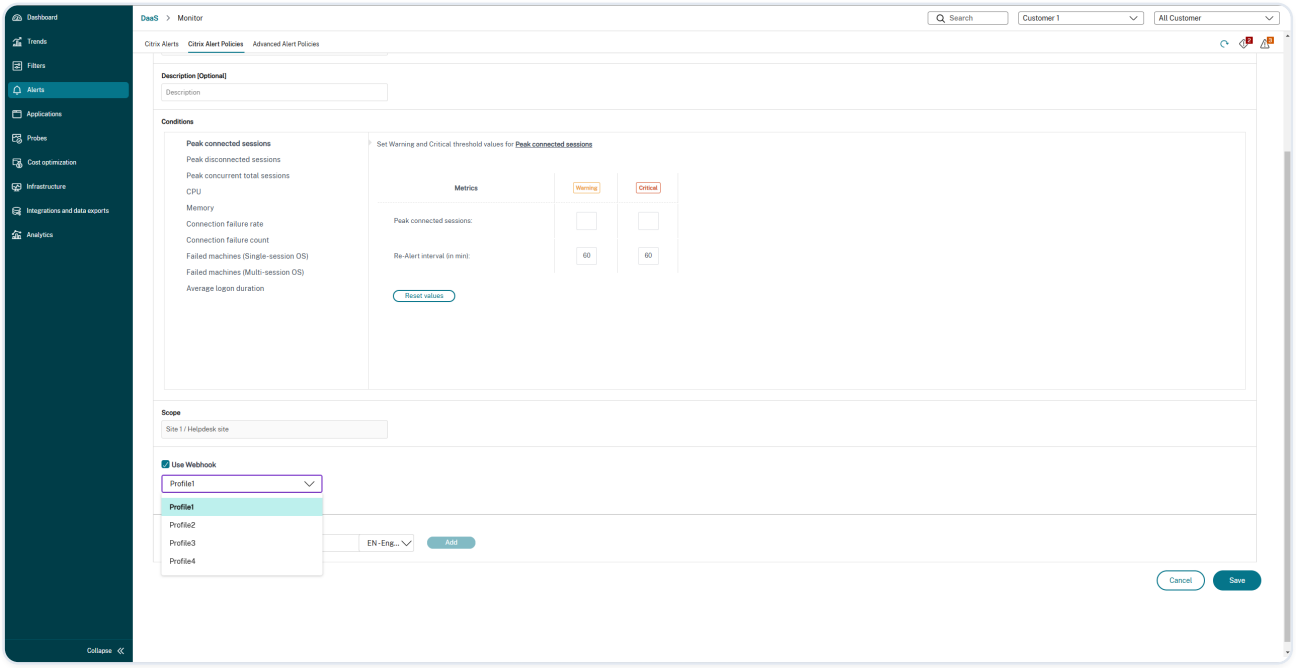
Exemplo:

```
PS C:\Users\administrator.STARWARS> $headers = [System.Collections.Generic.Dictionary[string,string]]::new()
PS C:\Users\administrator.STARWARS> $headers.Add("Content-Type", "application/json")
PS C:\Users\administrator.STARWARS> $headers.Add("Authorization", "Basic ************")
PS C:\Users\administrator.STARWARS> $payloads = '{ "text": "$PAYLOAD" }'
PS C:\Users\administrator.STARWARS> $url ="https://url.net"
PS C:\Users\administrator.STARWARS> Add-MonitorWebhookProfile -Name "webhookprofile1" -Description "Description" -Url $url -Headers $headers -PayloadFor
mat $payloads -Platform Slack -Type Webhook -MethodType POST
True
PS C:\Users\administrator.STARWARS>
PS C:\Users\administrator.STARWARS>
PS C:\Users\administrator.STARWARS> Get-MonitorWebhookProfile


Id            : 2
Name          : gg
Description   :
Url           : https://hooks.slack.com/triggers/<TeamId>/<WorkflowId>/<Token>
Headers       : {[Content-Type, application/json]}
PayloadFormat : { "text": "$PAYLOAD" }
MethodType    : POST
Type          : Webhook
Platform      : Slack

Id            : 3
Name          : webhookprofile1
Description   : Description
Url           : https://url.net
Headers       : {[Content-Type, application/json], [Authorization, Basic ************]}
PayloadFormat : { "text": "$PAYLOAD" }
MethodType    : POST
Type          : Webhook
Platform      : Slack
```

Depois que o perfil for criado, você poderá verificá-lo no banco de dados. Além disso, você pode encontrar o perfil de webhook recém-criado na página **Alertas do Citrix**.



Atualizar um perfil de webhook

Você pode usar o seguinte comando PowerShell de exemplo para atualizar um perfil de webhook:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")
```

```
$payloads = '{ "text": "$PAYLOAD" }'



$url =  "<Fill this field with the required URL>"



Set-MonitorWebhookProfile -Uid 1  -Name "profile_slack_citrix"
-Description "webhook profile for citrix slack" -Url $url -Headers
$headers -PayloadFormat $payloads -Platform Slack -Type Webhook
-MethodType POST
```

Exemplo:



Obter uma lista de todos os perfis de webhook

Você pode usar o seguinte comando de exemplo do PowerShell para obter uma lista de todos os perfis de webhook disponíveis:

```
Get-MonitorWebhookProfile



Get-MonitorWebhookProfile -Name 'profile_msteams'
```

```
Get-MonitorWebhookProfile -Uid 1
```

Remover um perfil de webhook

Você pode usar o seguinte comando de exemplo do PowerShell para remover um perfil de webhook:

```
Remove-MonitorWebhookProfile -Uid 1
```

Nota:

Se um perfil de webhook estiver mapeado para alguma política, ele não poderá ser removido. Como solução alternativa, você deve primeiro remover o mapeamento do webhook da política.

Criar uma política com perfil de webhook

Você pode usar o seguinte comando de exemplo do PowerShell para criar uma política com perfil de webhook:

```
New-MonitorNotificationPolicy -Name "Policy1" -Description "Policy
Description" -Enabled $true -WebhookProfileId 1
```

Atualizar uma política com perfil de webhook

Você pode usar o seguinte comando de exemplo do PowerShell para atualizar uma política com perfil de webhook:

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 1
```

Remover mapeamento de webhook de uma política

Você pode usar o seguinte comando de exemplo do PowerShell para remover o perfil de webhook de uma política:

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 0
```

Testar perfil de webhook

Você pode usar o seguinte comando de exemplo do PowerShell para testar o perfil de webhook:

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$headers.Add("Authorization", "Basic <Fill this with authorization
token>")


$payloads = '{ "text": "$PAYLOAD" }'


$url ="<Fill this field with the required URL>"


Test-MonitorWebhookProfile -Url $url -Headers $headers -PayloadFormat
$payloads
```

Monitoramento de alerta de falha de sincronização de configuração do Local Host Cache

O Cache de Host Local permite que as sessões de usuário continuem mesmo que os Cloud Connectors percam a conectividade com o Citrix Cloud. O cache usado pelo Cache de Host Local é sincronizado regularmente com o banco de dados primário para garantir configurações atualizadas quando o modo de Cache de Host Local é ativado. Você pode obter mais informações sobre o Cache de Host Local e o processo de sincronização de configuração em Cache de Host Local. Se a sincronização de configuração falhar mais de três vezes consecutivas, o Citrix Monitor envia um alerta de aviso ao administrador.

Uma política de alerta predefinida chamada **Cache de Host Local - Falha na Sincronização de Configuração** foi introduzida no Citrix Monitor para notificar os administradores sobre falhas na sincronização de configuração. Você pode encontrar a política recém-introduzida em **Monitor** >

Alertas do Citrix. Você pode modificar a política predefinida para adicionar ou editar destinatários de e-mail ou webhooks para receber notificações proativas em suas ferramentas de gerenciamento de alertas ou ITSM.

O escopo da política de alerta **Cache de Host Local - Falha na Sincronização de Configuração** é limitado apenas ao Site.

Monitoramento de Alertas de Hypervisor

O Monitor exibe alertas para monitorar a integridade do hypervisor. Alertas do Citrix Hypervisor™ e VMware vSphere ajudam a monitorar parâmetros e estados do hypervisor. O status da conexão com o hypervisor também é monitorado para fornecer um alerta se o cluster ou pool de hosts for reiniciado ou estiver indisponível.

Para receber alertas de hypervisor, certifique-se de que uma conexão de hospedagem seja criada na guia **Gerenciar**. Para obter mais informações, consulte Conexões e recursos. Somente essas conexões são monitoradas para alertas de hypervisor. A tabela a seguir descreve os vários parâmetros e estados dos alertas de Hypervisor.

ALERTA	HYPERVISORES SUPORTADOS	ACIONADO POR	CONDIÇÃO	CONFIGURAÇÃO
Uso da CPU	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso da CPU é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.
Uso de memória	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso de memória é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.
Uso de rede	Citrix Hypervisor, VMware vSphere	Hypervisor	O limite de alerta de uso de rede é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.

ALERTA	HYPERVISORES SUPORTADOS	ACIONADO POR	CONDIÇÃO	CONFIGURAÇÃO
Uso de disco	VMware vSphere	Hypervisor	O limite de alerta de uso de disco é atingido ou excedido	Os limites de alerta devem ser configurados no Hypervisor.
Conexão do host ou estado de energia	VMware vSphere	Hypervisor	O Host do Hypervisor foi reiniciado ou está indisponível	Os alertas são pré-construídos no VMware vSphere. Nenhuma configuração adicional é necessária.
Conexão do Hypervisor indisponível	Citrix Hypervisor, VMware vSphere	Delivery Controller	A conexão com o hypervisor (pool ou cluster) foi perdida, desligada ou reiniciada. Este alerta é gerado a cada hora enquanto a conexão estiver indisponível.	Os alertas são pré-construídos com o Delivery Controller. Nenhuma configuração adicional é necessária.

Nota:

Para obter mais informações sobre a configuração de alertas, consulte Alertas do Citrix XenCenter ou verifique a documentação de Alertas do VMware vCenter.

A preferência de notificação por e-mail pode ser configurada em **Citrix Alerts Policy > Site Policy > Hypervisor Health**. As condições de limite para as políticas de alerta do Hypervisor podem ser configuradas, editadas, desabilitadas ou excluídas apenas no hypervisor e não

> no Monitor. No entanto, a modificação das preferências de e-mail e o descarte de um alerta podem ser feitos no Monitor.

> **Importante:**
>
> - Todos os alertas de hipervisor com mais de um dia são automaticamente ignorados.
> - Os alertas acionados pelo Hipervisor são buscados e exibidos no Monitor. No entanto, as alterações no ciclo de vida/estado dos alertas do Hipervisor não são refletidas no Monitor.
> - Alertas que estão saudáveis, ignorados ou desabilitados no console do Hipervisor continuarão a aparecer no Monitor e devem ser ignorados explicitamente.
> - Alertas que são ignorados no Monitor não são ignorados automaticamente no console do Hipervisor.

> Filtro de Alertas do Hipervisor(/en-us/citrix-daas/media/hypervisor_alerts_filter.png)

Uma nova categoria de Alerta chamada **Integridade do Hipervisor** foi adicionada para permitir a filtragem apenas dos alertas do hipervisor. Esses alertas são exibidos assim que os limites são atingidos ou excedidos. Os alertas do hipervisor podem ser:

- Crítico — limite crítico da política de alarme do hipervisor atingido ou excedido
- Aviso — limite de aviso da política de alarme do hipervisor atingido ou excedido
- Ignorado — alerta não mais exibido como um alerta ativo

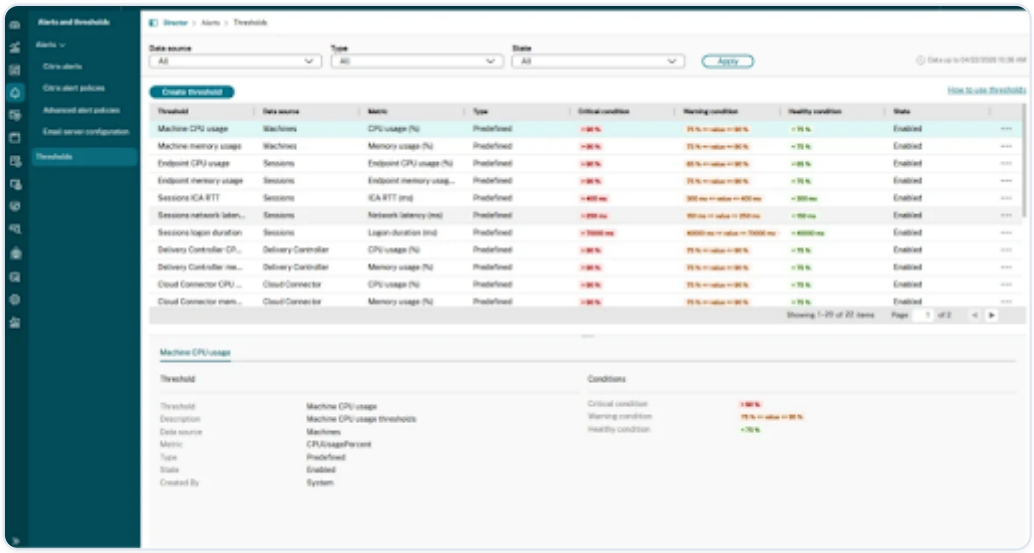
Exibição de Alertas do Hipervisor(/en-us/citrix-daas/media/hypervisor_alerts_display.png)

Limiares

Os limiares definem indicadores visuais de saúde para métricas do sistema em todo o console de monitoramento. Ao definir valores Crítico, Aviso e Saudável para cada métrica, os administradores podem identificar gargalos de desempenho através de indicadores codificados por cores em várias visualizações de painel.

Cada limiar se aplica a uma combinação específica de fonte de dados e métrica. O sistema inclui limiares predefinidos com base nas melhores práticas da Citrix e suporta limiares personalizados que podem ser adaptados às expectativas do ambiente. Os limiares habilitados aplicam

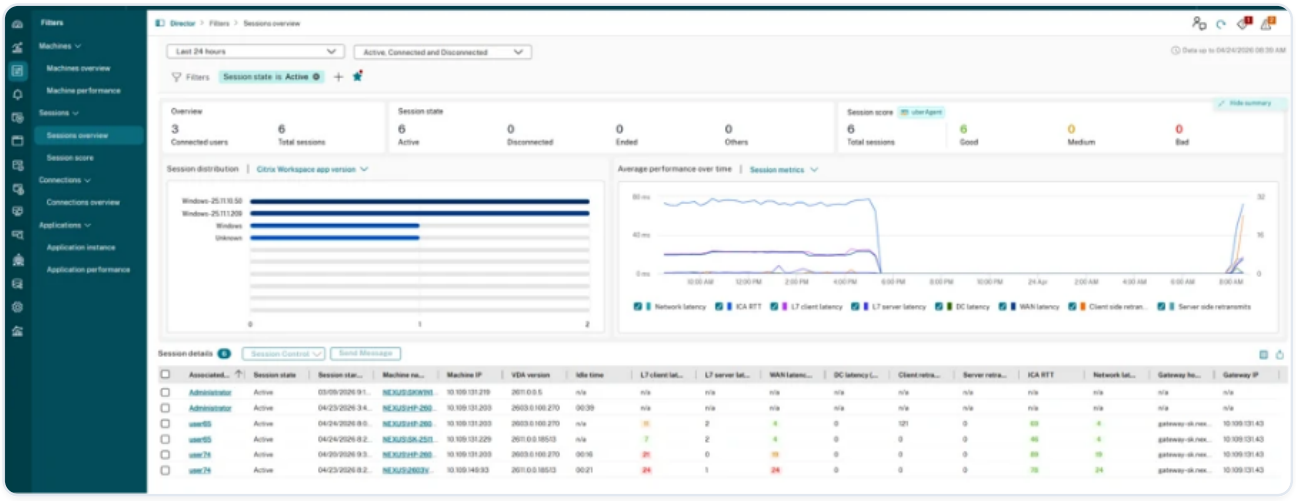
indicadores codificados por cores aos valores das métricas em todo o console, usando os valores Crítico, Aviso e Saudável definidos pelo administrador.



Os limiares atualizam os indicadores nas seguintes páginas:

- **Painel** — Duração do logon
- **Infraestrutura** — Status para Delivery Controllers, Cloud Connectors, Provisioning Services e StoreFront
- **Filtros** — Métricas de desempenho nas tabelas de Máquinas, Sessões, conexões e aplicativos
- **Detalhes do Usuário e Detalhes da Máquina** — Indicadores de métricas por usuário e por máquina





Pré-requisitos

- Citrix DaaS™ 129 ou Citrix Virtual Apps and Desktops™ 2611 ou posterior
- Permissões de administrador: Administrador completo ou administrador personalizado autorizado

Limiares predefinidos

Limites predefinidos são configurações geradas pelo sistema com base nas melhores práticas da Citrix. Estes não podem ser excluídos, mas podem ser editados ou desativados.

FONTE DE DADOS	MÉTRICA	VALOR CRÍTICO PADRÃO	VALOR DE AVISO PADRÃO	DINÂMICO
Máquinas	Uso da CPU %	90%	75%	Não
Máquinas	Uso da memória %	90%	75%	Não
Sessões	Uso da CPU %	90%	75%	Não
Sessões	Uso da memória %	90%	75%	Não
Endpoint de Sessões	Uso da CPU %	90%	75%	Não
Endpoint de Sessões	Uso de memória %	90%	75%	Não

FONTE DE DADOS	MÉTRICA	VALOR CRÍTICO PADRÃO	VALOR DE AVISO PADRÃO	DINÂMICO
Sessões	ICA RTT	400 ms	300 ms	Sim (P90/P70)
Sessões	Latência da rede	250 ms	150 ms	Sim (P90/P70)
Sessões	Duração do Logon	70.000 ms (70s)	40.000 ms (40s)	Sim (P90/P70)
Delivery Controller™	Uso da CPU %	90%	75%	Não
Delivery Controller	Uso da memória %	90%	75%	Não
Cloud Connector	Uso da CPU %	90%	75%	Não
Cloud Connector	Uso da memória %	90%	75%	Não
Serviço de provisionamento	Uso da CPU %	90%	75%	Não
Serviço de provisionamento	Uso de memória %	90%	75%	Não
StoreFront™	Uso de CPU %	90%	75%	Não
StoreFront	Uso de memória %	90%	75%	Não

Para redefinir um limite predefinido para as configurações padrão de fábrica, selecione o limite e escolha **Usar Padrão do Sistema**.

Limites personalizados

Limites personalizados são configurações criadas pelo administrador em todo o site. Ao contrário dos limites predefinidos, os limites personalizados podem ser totalmente excluídos.

Use limites personalizados para definir limites de métricas para ambientes onde os padrões predefinidos não correspondem às expectativas operacionais — por exemplo, um limite de RTT ICA mais rigoroso ou a utilização em VDAs.

Padrões dinâmicos

Para ICA RTT, Latência de Rede e Duração de Logon, o sistema calcula os valores padrão a cada sete dias com base nos dados de desempenho reais da semana anterior.

- **Aviso** — Definido no percentil 70 (P70): o valor abaixo do qual 70% das observações se enquadram.
- **Crítico** — Definido no percentil 90 (P90): o valor abaixo do qual 90% das observações se enquadram.

Os padrões dinâmicos permitem que os limites se adaptem automaticamente à linha de base da infraestrutura específica. As métricas são sinalizadas apenas quando excedem os níveis tipicamente experimentados pela maioria da base de usuários.

> **Nota:**
>
> Quando **Usar Padrão do Sistema** é selecionado para uma métrica dinâmica, o sistema gerencia os valores do limite automaticamente. Valores inseridos manualmente substituem os cálculos dinâmicos até que o limite seja redefinido.

Gerenciar limites

Criar um limite

navegar para **Limites** e selecione **Criar Limite**.

ETAPA 1: SELECIONAR FONTE DE DADOS E MÉTRICA

Selecione a fonte de dados (por exemplo, Máquinas, Sessões) e a métrica a ser monitorada.

ETAPA 2: DEFINIR VALORES DE LIMITE

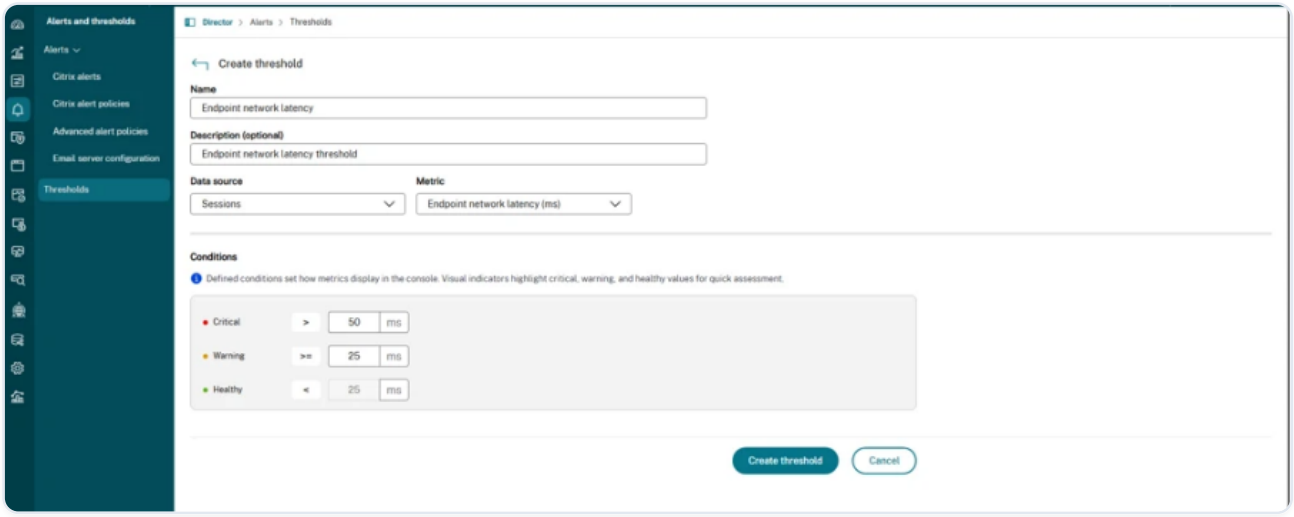
Insira valores para os estados Crítico e Aviso.

CAMPO	DESCRIÇÃO
Valor crítico	O valor acima do qual a métrica é sinalizada como Crítica (vermelho).

CAMPO	DESCRIÇÃO
Valor de aviso	O valor acima do qual a métrica é sinalizada como Aviso (âmbar).

ETAPA 3: SALVAR

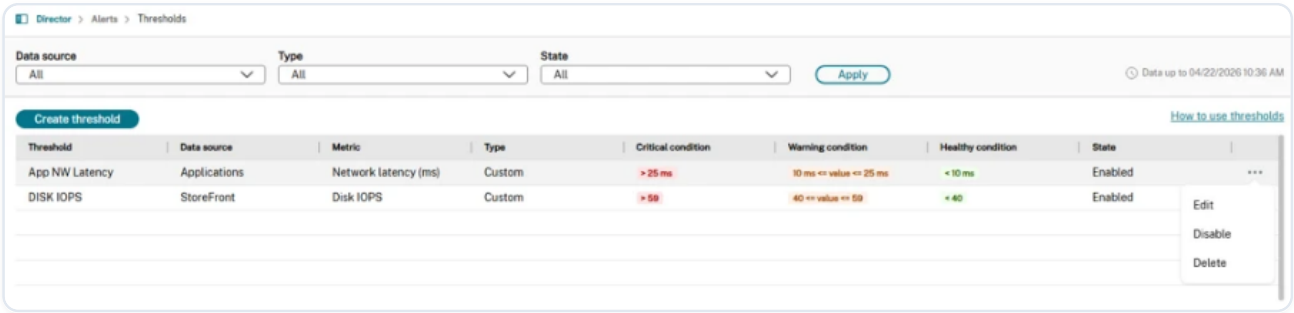
Selecione **Salvar** para ativar o limite. Indicadores codificados por cores aparecem nas páginas aplicáveis imediatamente.



Editar um limite

Selecione um limite na lista e escolha **Editar**. Modifique os valores Crítico ou Aviso e selecione **Salvar**.

Para limites predefinidos, selecione **Usar Padrão do Sistema** para reverter aos valores recomendados pela Citrix. Para métricas dinâmicas, isso reativa os cálculos automáticos de P70/P90.



Desativar um limite

Selecione um limite e escolha **Desativar**. Desativar um limite reverte a métrica para a formatação padrão em todas as páginas sem excluir a configuração. Reative o limite a qualquer momento para restaurar os indicadores codificados por cores.

Excluir um limite

Selecione um limite personalizado e escolha **Excluir**. Limites predefinidos não podem ser excluídos — desative-os em vez disso.

Solução de problemas

Valores padrão dinâmicos aparecem inesperadamente altos ou baixos

Solução: Os padrões dinâmicos refletem o P70 e o P90 dos sete dias anteriores de dados. Valores incomuns indicam um período de desempenho anormalmente alto ou baixo. Se os valores calculados não corresponderem às expectativas operacionais, edite o limite e insira valores manuais. Valores manuais substituem cálculos dinâmicos. Após uma semana de operações normais, redefina o limite para **Usar Padrão do Sistema** para recalcular.

Valores de limite predefinidos não correspondem aos padrões documentados

Solução: Um administrador pode ter editado o limite predefinido. Selecione o limite e escolha **Usar Padrão do Sistema** para restaurar os padrões de fábrica. Para métricas dinâmicas (ICA RTT, Latência de Rede, Duração de Logon), os valores são recalculados semanalmente. Os valores atuais refletem o cálculo P70/P90 mais recente, não os padrões estáticos listados na tabela acima.

Monitoramento do uso de aplicativos

O Citrix Monitor ajuda você a monitorar o uso de aplicativos iniciados diretamente da sessão do aplicativo Citrix Workspace™ (também conhecidos como aplicativos publicados)

O relatório de uso de aplicativos fornece visibilidade sobre os aplicativos mais, menos e não utilizados. Os aplicativos mais usados são apresentados no Painel e contêm gráficos selecionados. Esses gráficos ajudam os administradores de TI ou administradores de aplicativos a obter informações sobre quais aplicativos são muito usados e a extensão de seu uso.

> **Nota:**

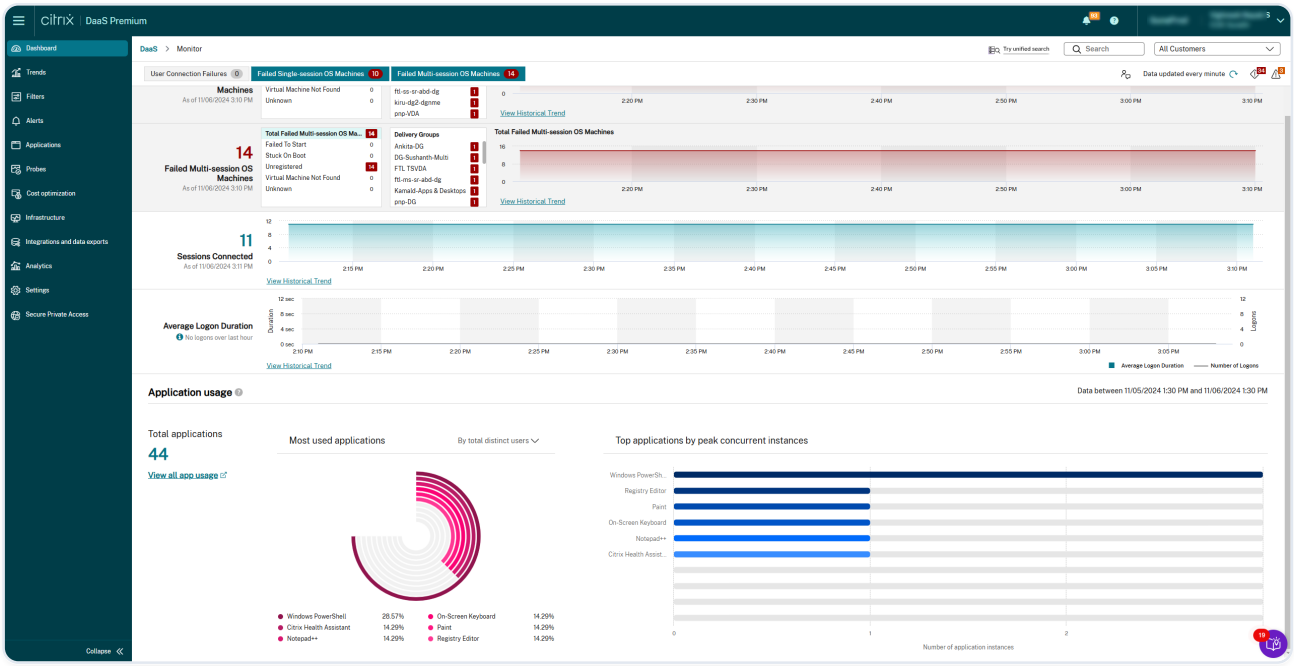
> Este recurso está disponível apenas para sites com licença platinum.

> Com este recurso, um administrador pode ver quais aplicativos publicados são os mais usados. Usando esses dados, os administradores podem aprofundar-se na extensão do uso.

> O administrador pode analisar os detalhes dos aplicativos populares nas últimas 24 horas pelos seguintes pontos de dados:

- Número total de aplicativos - Identifica o número total de aplicativos em uso por todos os usuários no site da empresa.
- Aplicativos mais usados pelo número total de usuários distintos - Identifica os 10 principais aplicativos pelo número total de usuários únicos.
- Aplicativos mais usados pelo número total de inicializações de aplicativos - Identifica os 10 principais aplicativos com base no número total de inicializações de aplicativos.
- Principais instâncias de aplicativos simultâneas de pico - Identifica os 10 principais aplicativos com base no maior número de instâncias simultâneas de uso de cada aplicativo. Esta informação fornece a demanda máxima para os aplicativos listados.

Este gráfico está presente na parte inferior da página do Painel. No entanto, você pode clicar em **Confira** na parte superior da tela para acessar o gráfico diretamente.



Você também pode clicar em **Ver todo o uso do aplicativo** para ver os detalhes de um único aplicativo. Este link abre a página **Tendências** > **Gerenciamento de Capacidade** > **Uso de Aplicativos Hospedados**.

O gráfico fornece uma representação visual do uso do aplicativo. Além disso, ao passar o mouse sobre o gráfico, você obtém as contagens absolutas respectivas dos pontos de dados selecionados. Ao clicar em qualquer ponto de dados no gráfico, a página **Tendências** > **Gerenciamento de Capacidade** > **Uso de Aplicativos Hospedados** é aberta com o nome do aplicativo específico selecionado. Esses dados servem para representar um valor comparativo em

relação a todos os aplicativos presentes no sistema da empresa. O valor absoluto do ponto de dados também é mencionado separadamente no mesmo hover.

Relatório de aplicativos menos usados e não usados

Em um ambiente Citrix DaaS™ grande, é comum ter muitos aplicativos subutilizados. Para otimizar seu ambiente, a página **Aplicativos** agora oferece métricas extras para ajudar você a entender os padrões de uso de aplicativos dentro da organização e tomar decisões baseadas em dados para melhorar a alocação de recursos e a economia de custos.

Principais recursos

- **Informações detalhadas de uso:** Visualize usuários distintos (últimos 30 dias), lançamentos totais, instâncias simultâneas de pico e um gráfico de tendências de usuários distintos ao longo do tempo para cada aplicativo.
- **Foco nos dados:** Analise os padrões de uso de aplicativos nos últimos sete dias, 30 dias ou 90 dias para avaliar a necessidade do aplicativo. A visualização de dados por 90 dias é recomendada, pois fornece dados de um trimestre, permitindo observar se o uso do aplicativo flutua ou permanece consistente. As datas no eixo X ajudam a correlacionar eventos organizacionais com tendências de uso para determinar se uma queda era esperada. Esses dados capacitam os administradores a manter ambientes eficientes, eliminando aplicativos desnecessários.
- **Otimização:** Identifique o total de aplicativos publicados, aplicativos menos usados e aplicativos não usados para otimizar sua implantação Citrix.
- **Dados acionáveis:** Tome decisões baseadas em dados que auxiliam no gerenciamento de aplicativos para otimizar a alocação de recursos e o gerenciamento de licenças.
- **Exportar dados:** Exporte dados nos formatos PDF ou CSV para análise posterior. Você também pode exportar os dados usando a integração do Power BI ou consultas ODATA usando o uso do aplicativo.

> **Observação:**
>
> Atualmente, apenas aplicativos publicados (referidos como aplicativos de desktop no aplicativo Citrix Workspace) estão incluídos nesta melhoria.

Requisitos

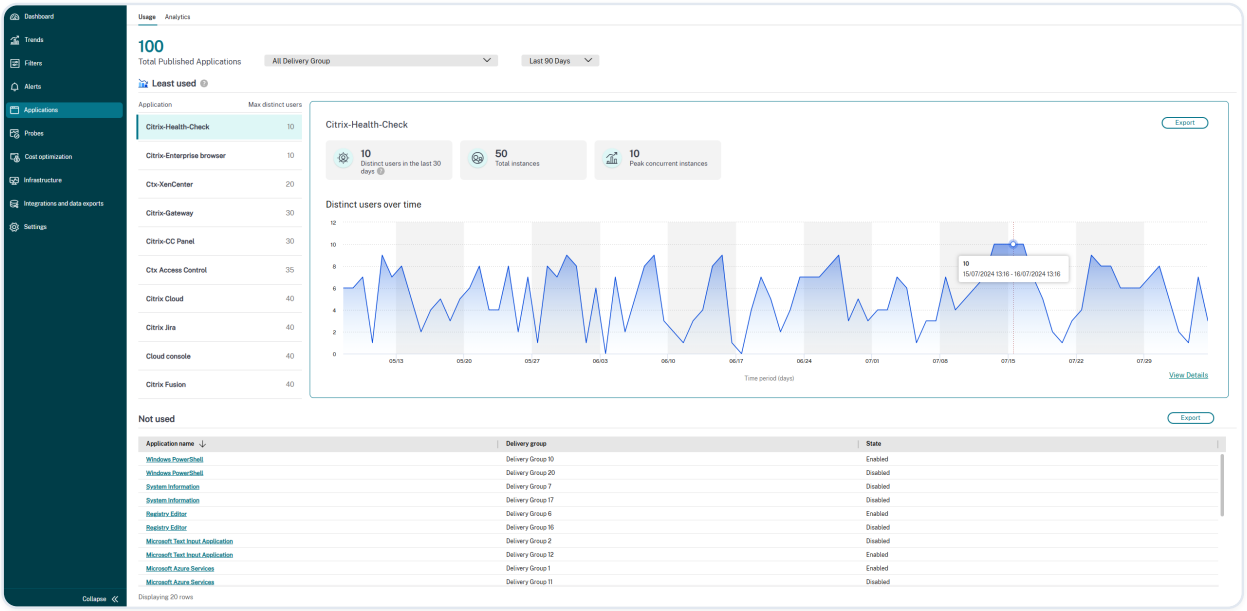
- VDAs versão 7.15 ou posterior

Visualizando detalhes de uso de aplicativos

1. Clique no link **Visualizar aplicativos** na seção **Revisar aplicativos menos usados** no Painel.

   Ou,

   Clique na guia **Aplicativos**. A seguinte página é exibida:



2. Selecione o grupo de entrega desejado.
3. Selecione o período de tempo necessário. (Observação: Para uma análise ideal, o padrão são os últimos 90 dias.)

   As seguintes informações são exibidas:

   - **Total de aplicativos publicados:** Exibe o número total de aplicativos publicados.
   - **Menos usados:** Exibe os aplicativos com o menor número de usuários únicos durante o período selecionado. O cálculo é feito da seguinte forma:

     a. **Contagem diária de usuários:** O número de usuários únicos para cada aplicativo é contado diariamente.

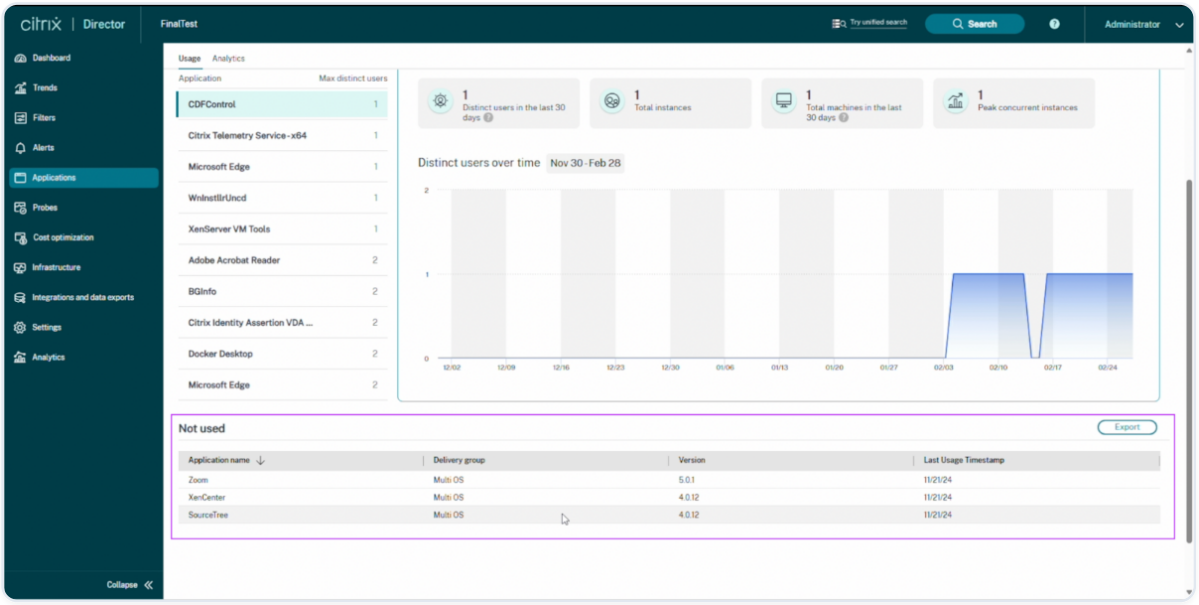
     b. **Pico de uso diário:** A maior contagem diária de usuários para cada aplicativo é identificada.

     c. **Maior uso geral:** A maior contagem de usuários para cada aplicativo no período selecionado é determinada.

     d. **Ordem crescente:** Os aplicativos são listados em ordem crescente com base na maior contagem geral de usuários, começando com o aplicativo com a menor contagem de usuários.

> **Observação:**
>
> Recomenda-se selecionar os últimos 90 dias como período para análise. Esse intervalo de dias fornece dados de um trimestre e oferece uma visão abrangente dos padrões de uso de aplicativos. No entanto, opções para filtrar por sete dias e um mês também estão disponíveis.

- **Não usados:** Exibe os aplicativos que não foram iniciados nenhuma vez nos últimos 90 dias. São fornecidos o grupo de entrega pelo qual foram entregues, a versão do aplicativo e o carimbo de data/hora exato de seu último uso. Essas informações ajudam os administradores a tomar decisões informadas antes de remover um aplicativo de um desktop virtual.



4. Selecione um aplicativo da categoria **Menos usados** para visualizar informações detalhadas de uso, incluindo:

   - **Usuários distintos nos últimos 30 dias:** Exibe o número de usuários distintos que acessaram o aplicativo nos últimos 30 dias. Se você filtrar por sete dias, essa métrica mostra o número distinto de usuários para o aplicativo selecionado durante esses sete dias.

> **Nota:**
>
> Mesmo quando você seleciona 90 dias, esta métrica ainda exibe dados apenas dos últimos 30 dias.

- **Total de inicializações:** Mostra o número de vezes que o aplicativo foi inicializado.
- **Pico de instâncias simultâneas:** Exibe o maior número de instâncias sendo executadas simultaneamente.
- **Gráfico de tendências:** Visualize um gráfico de tendências mostrando o número de usuários distintos ao longo do tempo para o aplicativo selecionado. Clique em **Ver detalhes** para ver mais informações na seção **Gerenciamento de Capacidade > Uso de Aplicativos Hospedados**.

Uso do gráfico de tendências

O gráfico de tendências ilustra os padrões de uso, ajudando a identificar tendências e períodos de baixo ou alto uso durante o período selecionado. O eixo X representa o período em dias, e o eixo Y representa o número de usuários distintos ao longo do tempo. Ao analisar essas métricas e o gráfico de padrões de uso, os administradores podem otimizar com confiança seu ambiente Citrix DaaS.

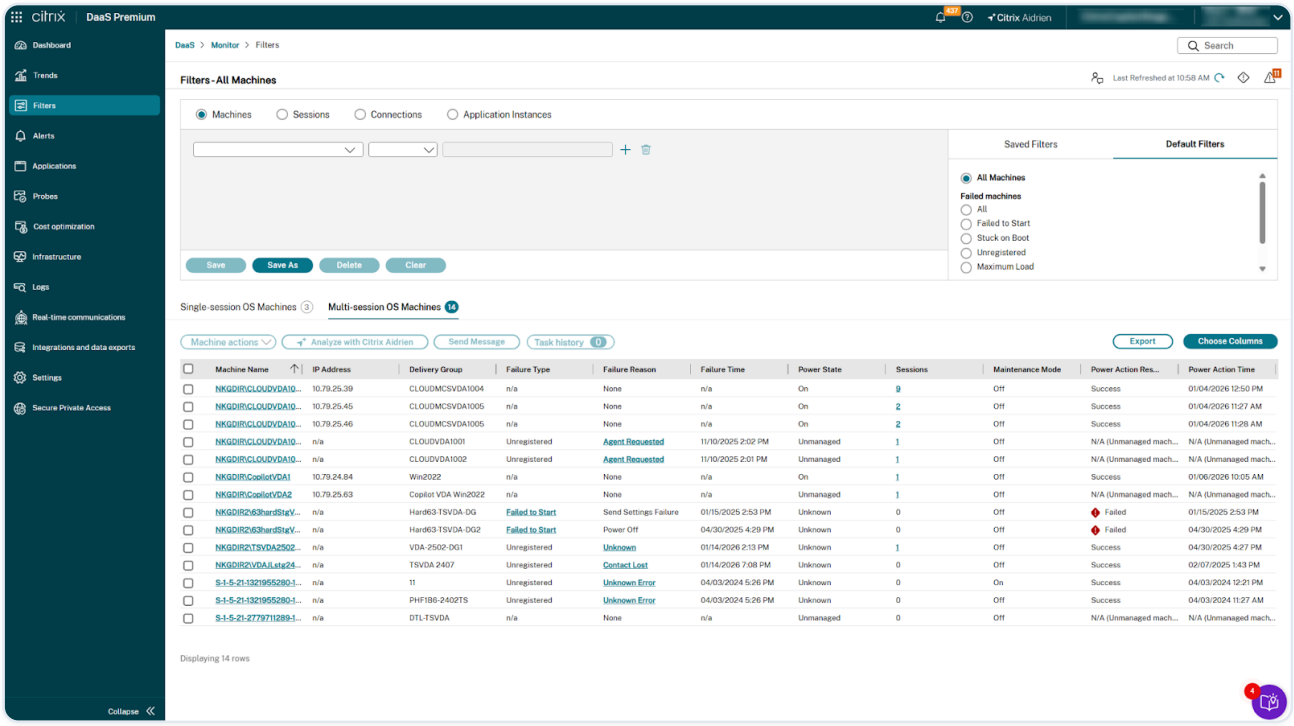
Você pode usar o gráfico de tendências das seguintes maneiras:

- **Passe o mouse sobre os pontos de dados:** Visualize o número de usuários distintos para o período selecionado.
- **Ver tendências:** Identifique padrões de uso e determine se o uso do aplicativo é consistente ou apenas um pico temporário. Este gráfico é útil para os administradores monitorarem a atividade dos funcionários e identificarem possíveis problemas ou áreas de melhoria. Por exemplo, se um funcionário sai de férias, pode não haver uso do aplicativo durante esse período. Assim que o funcionário retorna, o uso do aplicativo aumenta. O filtro padrão para o período é de 90 dias, o que auxilia os administradores a fazer esses cálculos.
- **Ver detalhes:** Veja a data e o número correspondente de usuários distintos.
- **Opções de filtro:** Selecione diferentes opções de filtro de Período de Tempo para visualizar os dados correspondentes.

Filtrar dados para solucionar falhas

Quando você clica em números no Painel ou seleciona um filtro Padrão predefinido na guia **Filtros**, a exibição Filtros é aberta para exibir dados com base na máquina ou tipo de falha selecionado.

Você pode criar exibições filtradas personalizadas de máquinas, conexões, sessões e instâncias de aplicativos em todos os grupos de entrega e salvar a pesquisa para acesso posterior. Você pode editar um filtro predefinido e salvá-lo como um filtro Salvo.



1. Selecione uma exibição:

   - **Máquinas**. Selecione Máquinas de SO de sessão única ou Máquinas de SO de várias sessões. Essas exibições mostram o número de máquinas configuradas. A guia Máquinas de SO de várias sessões também inclui o índice do avaliador de carga, que indica a distribuição de contadores de desempenho e dicas de ferramentas da contagem de sessões se você passar o mouse sobre o link.
   - **Sessões**. Você também pode ver a contagem de sessões na exibição Sessões. Use as medições de tempo ocioso para identificar sessões que estão ociosas além de um período de tempo limite. Clique em **Usuário Associado** para abrir o Gerenciador de Atividades para o usuário. Clicar no nome do **Endpoint** abre o Gerenciador de Atividades para o Endpoint. Clicar em **Exibir Detalhes** abre a página **Detalhes do Usuário** ou **Detalhes do Endpoint**, respectivamente. Para obter mais informações, consulte Detalhes do Usuário.
   - **Conexões**. Filtre as conexões por diferentes períodos de tempo, incluindo os últimos 60 minutos, as últimas 24 horas ou os últimos 7 dias. Clique em **Usuário Associado** para abrir o Gerenciador de Atividades para o usuário. Clicar no nome do **Endpoint** abre o Gerenciador de Atividades para o Endpoint. Clicar em **Nomes de Máquina** abre a página Detalhes da Máquina. A página **Detalhes da Máquina** lista os detalhes da máquina,

utilização da máquina, detalhes da infraestrutura e hotfixes aplicados. Para obter mais informações, consulte Solucionar problemas de máquinas.

- **Instâncias de Aplicativo**. Esta exibição mostra as propriedades de todas as instâncias de aplicativo em VDAs de SO de várias sessões e de sessão única. As medições de tempo ocioso da sessão estão disponíveis para instâncias de aplicativo em VDAs de SO de várias sessões.

2. Selecione um filtro na lista de filtros Salvos ou Padrão.
3. Use as listas suspensas para selecionar outros critérios de filtro.
4. Selecione colunas extras, conforme necessário, para solucionar problemas adicionais.
5. Salve e nomeie seu filtro.
6. Para abrir o filtro mais tarde, na exibição Filtros, selecione Exibição (Máquinas, Sessões, Conexões ou Instâncias de Aplicativo) e selecione o filtro salvo.
7. Clique em **Exportar** para exportar os dados para arquivos no formato CSV. Dados de até 100.000 registros podem ser exportados.
8. Se necessário, para as exibições de **Máquinas** ou **Conexões**, use as ações da máquina para todas as máquinas selecionadas na lista filtrada. Para a exibição de Sessões, use os controles de sessão ou a opção para enviar mensagens.

> **Nota:**
>
> - A execução de Tarefa de Script (Run Scripted Task) é suportada apenas quando o serviço WEM (Workspace Environment Management) é provisionado e o agente WEM no VDA está instalado e registrado no serviço WEM.
> - O Histórico de Tarefas (Task History) mostra apenas as execuções de Tarefas de Script (Scripted Task) do usuário atual nas últimas 24 horas.

9. Se necessário, você pode usar várias ações. Você recebe uma barra de progresso sobre o andamento da ação. Além disso, recebe uma mensagem quando a ação é concluída.
10. Nas exibições de **Máquinas** e **Conexões**, clique em **Motivo da Falha** de uma máquina ou conexão com falha para obter uma descrição detalhada da falha e as ações recomendadas para solucionar o problema. Os motivos da falha e as ações recomendadas para falhas de Máquina e Conexão estão disponíveis no Guia de Solução de Problemas de Motivos de Falha do Citrix Director.

11. Na exibição de **Máquinas**, clique em um link de nome de máquina para ir para a página correspondente de **Detalhes da Máquina**. Esta página exibe os detalhes da máquina, fornece controles de energia, exibe os gráficos de monitoramento de CPU, memória, disco e GPU. Além disso, clique em **Exibir Utilização Histórica** para ver as tendências de utilização de recursos da máquina. Para obter mais informações, consulte Solucionar problemas de máquinas.
12. Na exibição de **Instâncias de Aplicativo**, classifique ou filtre com base no **Tempo Ocioso** maior que um período de tempo limite. Selecione as instâncias de aplicativo ociosas para encerrar. O Logoff ou Desconexão de uma instância de aplicativo encerra todas as instâncias de aplicativo ativas na mesma sessão. Para obter mais informações, consulte Solucionar problemas de aplicativos. A página de filtro de Instâncias de Aplicativo e as medições de tempo ocioso nas páginas de filtro de Sessões estão disponíveis se os VDAs forem da versão 7.13 ou posterior.

Nota:

O Studio permite a atribuição de várias Regras de Atribuição de Desktop (DAR) para diferentes usuários ou grupos de usuários a um único VDA no grupo de entrega. O StoreFront exibe o desktop atribuído com o Nome de Exibição correspondente de acordo com a DAR para o usuário logado. No entanto, o Monitor não suporta DARs e exibe o desktop atribuído usando o nome do grupo de entrega, independentemente do usuário logado. Como resultado, você não pode mapear um desktop específico para uma máquina no Monitor. Para mapear o desktop atribuído exibido no StoreFront para o nome do grupo de entrega exibido no Monitor, use o seguinte comando PowerShell. Execute o comando PowerShell usando o SDK do PowerShell Remoto, conforme descrito no blog.

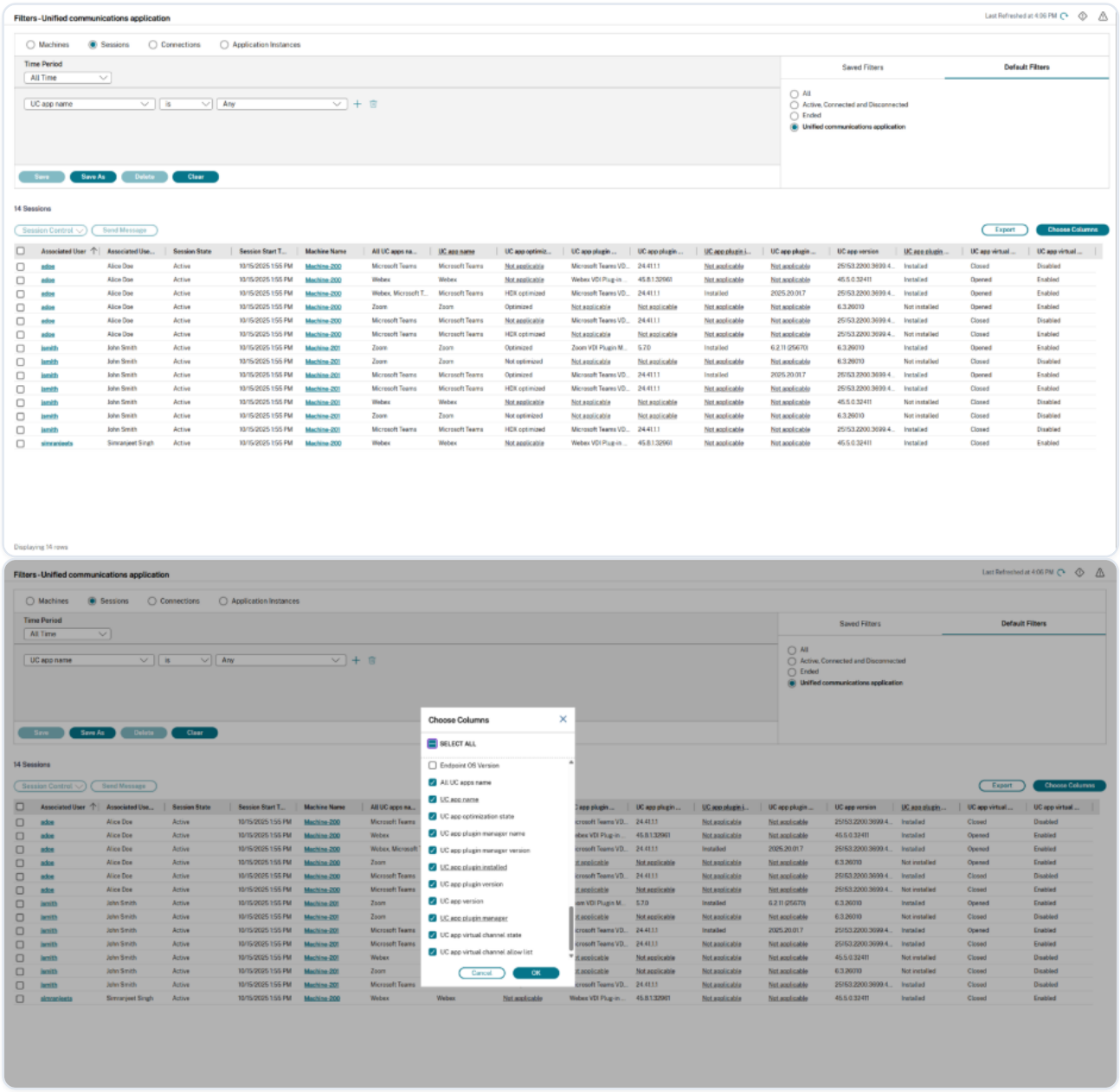
```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

Métricas de aplicativos de Comunicação Unificada

A exibição de **Sessões** agora inclui várias novas colunas de exibição que fornecem insights detalhados sobre o uso de aplicativos de Comunicações Unificadas (UC) para uma sessão de usuário. Essas métricas estão disponíveis no filtro para refinar a lista de sessões e também

podem ser selecionadas através da opção **Escolher Colunas** para serem exibidas na visualização da tabela principal de sessões.

- **Nome de todos os aplicativos UC (Somente Coluna)**: Contém a listagem de dados para todos os múltiplos aplicativos UC que estavam sendo executados na sessão simultaneamente. Esta é uma coluna de exibição e não uma opção de filtro.
- **Nome do aplicativo UC**: O nome do aplicativo específico de Comunicações Unificadas (por exemplo, Microsoft Teams, Webex, Zoom).
- **Estado de otimização do aplicativo UC**: O status de otimização do aplicativo UC dentro da sessão (por exemplo, Otimizado, otimizado para HDX, não otimizado, não aplicável).
- **Nome do gerenciador de plug-ins do aplicativo UC**: O nome do gerenciador de plug-ins usado para o aplicativo UC.
- **Versão do gerenciador de plug-ins do aplicativo UC**: A versão do gerenciador de plug-ins em uso.
- **Plug-in do aplicativo UC instalado**: Indica se o plug-in do aplicativo necessário está Instalado ou Não instalado para o aplicativo UC.
- **Versão do plug-in do aplicativo UC**: A versão do plug-in específico do aplicativo UC.
- **Versão do aplicativo UC**: A versão geral do aplicativo de Comunicações Unificadas.
- **Gerenciador de plug-ins do aplicativo UC**: Indica se o gerenciador de plug-ins do aplicativo necessário está Instalado ou Não instalado no endpoint para o aplicativo UC.
- **Estado do canal virtual do aplicativo UC**: O status do canal virtual estabelecido para o aplicativo UC (por exemplo, Aberto, Fechado).
- **Lista de permissões do canal virtual do aplicativo UC**: Indica se o canal virtual do aplicativo está na lista de permissões.



Monitorar tendências históricas em um site

A exibição Tendências acessa informações de tendências históricas de cada site para os seguintes parâmetros:

- sessões
- falhas de conexão
- falhas de máquina
- desempenho de logon
- avaliação de carga
- gerenciamento de capacidade

- uso da máquina
- utilização de recursos

Para localizar essas informações, clique no menu **Tendências**.

O recurso de detalhamento com zoom permite que você navegar pelos gráficos de tendências, ampliando um período de tempo (clicando em um ponto de dados no gráfico) e detalhando para ver os detalhes associados à tendência. Esse recurso permite que você entenda melhor os detalhes de quem ou o que foi afetado pelas tendências exibidas.

Para alterar o escopo padrão de cada gráfico, aplique um filtro diferente aos dados.

> **Nota:**
>
> - As informações de tendência de sessões, falhas e desempenho de logon estão disponíveis como gráficos e tabelas quando o período de tempo é definido como Último mês (**Terminando agora**) ou menor. Quando o período de tempo é escolhido como Último mês com uma data de término personalizada ou como Último ano, as informações de tendência estão disponíveis como gráficos, mas não como tabelas.
> - O Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™) oferece suporte à retenção de dados históricos por apenas 90 dias. Portanto, as tendências e relatórios de um ano no Monitor mostram os dados dos últimos 90 dias.

Tendências disponíveis

Exibir tendências para sessões: Na guia Sessões, selecione o grupo de entrega e o período para exibir informações mais detalhadas sobre a contagem de sessões simultâneas.

A coluna **Reconexão Automática de Sessão** exibe o número de reconexões automáticas em uma sessão. A reconexão automática é ativada quando as políticas de Confiabilidade da Sessão ou Reconexão Automática do Cliente estão em vigor. Quando há uma interrupção de rede no endpoint, as seguintes políticas entram em vigor:

- A confiabilidade da sessão entra em vigor (por padrão por 3 minutos) onde o Citrix Receiver™ ou o aplicativo Citrix Workspace™ tenta se conectar ao VDA.
- A reconexão automática do cliente entra em vigor entre 3 e 5 minutos, onde o cliente tenta se conectar ao VDA.

Ambas as reconexões são capturadas e exibidas ao usuário. Essas informações podem levar no máximo 5 minutos para aparecer na interface do usuário do Monitor após a reconexão ocorrer.

As informações de reconexão automática ajudam você a visualizar e solucionar problemas de conexões de rede com interrupções e a analisar redes com uma experiência perfeita. Você pode visualizar o número de reconexões para um grupo de entrega específico ou período selecionado nos Filtros.

Um detalhamento fornece informações adicionais como Confiabilidade da Sessão ou Reconexão Automática do Cliente, carimbos de data/hora, IP do Endpoint e Nome do Endpoint da máquina onde o aplicativo Workspace está instalado.

Por padrão, os logs são classificados pelos carimbos de data/hora do evento em ordem decrescente. Este recurso está disponível para Citrix Workspace app para Windows, Citrix Workspace app para Mac, Citrix Receiver para Windows e Citrix Receiver para Mac. Este recurso requer VDAs 1906 ou posterior.

Para obter mais informações sobre reconexões de sessão, consulte Sessões. Para obter mais informações sobre políticas, consulte Configurações da política de reconexão automática do cliente e Configurações da política de confiabilidade da sessão.

Às vezes, os dados de reconexão automática podem não aparecer no Monitor pelos seguintes motivos:

- O aplicativo Workspace não está enviando dados de reconexão automática para o VDA.
- O VDA não está enviando dados para o serviço Monitor.

> **Nota:**
>
> Às vezes, o endereço IP do cliente pode não ser obtido corretamente se certas políticas do Citrix Gateway estiverem definidas.

> **Exibir tendências para falhas de conexão:** Na guia Falhas, selecione a conexão, o tipo de máquina, o tipo de falha, o grupo de entrega e o período para exibir um gráfico contendo informações mais detalhadas sobre as falhas de conexão do usuário em seu site.

Exibir tendências para falhas de máquina: Na guia Falhas de Máquina OS de Sessão Única ou na guia Máquinas OS de Múltiplas Sessões, selecione o tipo de falha, o grupo de entrega e o

período para exibir um gráfico contendo informações mais detalhadas sobre as falhas de máquina em seu site.

Exibir tendências para o desempenho de logon: Na guia Desempenho de Logon, selecione o grupo de entrega e o período para exibir um gráfico contendo informações mais detalhadas sobre a duração dos tempos de logon do usuário em seu site e se o número de logons afeta o desempenho. Esta exibição também mostra a duração média das fases de logon, como a duração do agenciamento e o tempo de inicialização da VM. Esses dados são especificamente para logons de usuário e não incluem usuários tentando se reconectar de sessões desconectadas. A tabela abaixo do gráfico mostra a Duração do Logon por Sessão do Usuário. Você pode escolher as colunas a serem exibidas e classificar o relatório por qualquer uma das colunas. Você também pode exportar esses relatórios para um arquivo .CSV. Para obter mais informações, consulte Diagnosticar problemas de logon do usuário.

Exibir tendências para avaliação de carga: Na guia Índice do Avaliador de Carga, exiba um gráfico contendo informações mais detalhadas sobre a carga distribuída entre as máquinas OS de múltiplas sessões. As opções de filtro para este gráfico incluem o grupo de entrega ou a máquina OS de múltiplas sessões em um grupo de entrega, a máquina OS de múltiplas sessões (disponível apenas se uma máquina OS de múltiplas sessões em um grupo de entrega foi selecionada) e o intervalo. O Índice do Avaliador de Carga é exibido como porcentagens de CPU Total, Memória, Disco ou Sessões e é mostrado em comparação com o número de usuários conectados no último intervalo.

Exibir tendências para cache de host local: Na guia **Cache de Host Local**, selecione o período, a zona e o conector de nuvem para exibir as informações detalhadas sobre os dados perdidos durante a interrupção, como o número de máquinas registradas, o número de máquinas reconectadas e o número de sessões agenciadas em seu site. Os dados exibidos são baseados no período, zona e conector de nuvem selecionados.

Você também pode visualizar dados para todas as zonas e conectores de nuvem. Os dados selecionados por padrão são para as últimas 24 horas e para todas as zonas e conectores de nuvem. Os dados do cache de host local estão disponíveis para as últimas 2 horas, 24 horas, 7 dias, mês e 90 dias. O máximo de dados disponível é para os últimos 90 dias. Para obter mais informações sobre o cache de host local, consulte a documentação Cache de Host Local. A exibição mostra os seguintes dados de cache de host local por zona e conector de nuvem selecionados para o período selecionado:

- Hora de início da interrupção
- Hora de término da interrupção

- Duração da interrupção
- Novas sessões agenciadas durante a interrupção
- Número de sessões reconectadas durante a interrupção
- Número de máquinas registradas durante a interrupção
- Número de máquinas afetadas durante a interrupção
- O nome da zona
- O nome do conector de nuvem

Visualizar uso de aplicativos hospedados: Na guia Gerenciamento de Capacidade, selecione a guia Uso de Aplicativos Hospedados, selecione o grupo de entrega e o período para visualizar um gráfico exibindo o pico de uso simultâneo e uma tabela exibindo o uso baseado em aplicativo. Na tabela Uso Baseado em Aplicativo, você pode escolher um aplicativo específico para ver detalhes e uma lista de usuários que estão usando ou usaram o aplicativo.

Visualizar uso de SO de sessão única e multissessão: A exibição Tendências mostra o uso de SO de sessão única por site e por grupo de entrega. Quando você seleciona o site, o uso é mostrado por grupo de entrega. Quando você seleciona o grupo de entrega, o uso é mostrado por Usuário. A exibição Tendências também mostra o uso de SO multissessão por site, por grupo de entrega e por Máquina. Quando você seleciona o site, o uso é mostrado por grupo de entrega. Quando você seleciona o grupo de entrega, o uso é mostrado por Máquina e por Usuário. Quando a Máquina é selecionada, o uso é mostrado por Usuário.

Visualizar uso de máquina virtual: Na guia **Uso da Máquina**, selecione **Máquinas de SO de sessão única** ou **Máquinas de SO multissessão** para obter uma visualização em tempo real do uso da sua VM. A página exibe o número de máquinas de SO multissessão e de sessão única habilitadas para Autoscale™ que estão ligadas para um grupo de entrega e período selecionados. Também estão disponíveis as economias estimadas alcançadas ao habilitar o Autoscale no grupo de entrega selecionado. Essa porcentagem é calculada usando os custos por máquina.

As tendências de uso das máquinas habilitadas para Autoscale indicam o uso real das máquinas, permitindo que você avalie rapidamente as necessidades de capacidade do seu site.

- Disponibilidade de SO de sessão única - exibe o estado atual das máquinas de SO de sessão única (VDIs) por disponibilidade para todo o site ou um grupo de entrega específico.
- Disponibilidade de SO multissessão - exibe o estado atual das máquinas de SO multissessão por disponibilidade para todo o site ou um grupo de entrega específico.

Você pode clicar nos seguintes links no banner exibido para obter melhor visibilidade do uso da máquina com a Otimização de Custos:

- Economias estimadas - Este link direciona você para a seção **Economias estimadas** na página **Otimização de custos**, exibindo detalhes de todos os grupos de entrega.
- Relatório de economias - Este link direciona você para a seção **Relatório de economias** na página **Otimização de custos**, exibindo detalhes de todos os grupos de entrega.

> **Nota:**
>
> A grade abaixo do gráfico exibe os dados de uso da máquina baseados no grupo de entrega em tempo real. Os dados incluem a disponibilidade da máquina de todas as máquinas, independentemente da habilitação do Autoscale. O número de máquinas exibidas na coluna Contador Disponível na grade inclui máquinas em modo de manutenção.

> A consolidação dos dados de monitoramento depende do período que você selecionar.

- Os dados de monitoramento para os períodos de um dia e uma semana são consolidados por hora.
- Os dados de monitoramento para o período de um mês são consolidados por dia.

O status da máquina é lido no momento da consolidação e quaisquer alterações durante o período intermediário não são consideradas. Para o período de consolidação, consulte a documentação da API do Monitor.

Para obter mais informações sobre o monitoramento de máquinas com Autoscale ativado, consulte o artigo Autoscale.

Visualizar utilização de recursos: Na guia **Utilização de Recursos**, selecione **Máquinas OS de sessão única ou Máquinas OS de várias sessões** para obter informações sobre dados de tendências históricas para uso de CPU e memória, e IOPS e latência de disco para cada máquina VDI para um melhor planejamento de capacidade. Este recurso requer VDAs **versão 7.11** ou posterior. Os gráficos mostram dados para CPU média, memória média, IOPS médio, latência de disco e sessões simultâneas de pico. Você pode detalhar a máquina e visualizar dados e gráficos para os 10 principais processos que consomem CPU. Filtre por grupo de entrega e período de tempo. Os gráficos de CPU, uso de memória e sessões simultâneas de pico estão disponíveis

para as últimas 2 horas, 24 horas, 7 dias, mês e ano. Os gráficos de IOPS médio e latência de disco estão disponíveis para as últimas 24 horas, mês e ano.

Você pode clicar no **link desproteger** no banner para obter melhor visibilidade do uso da máquina com a Otimização de custos. Este link leva você à guia **Dimensionamento de carga de trabalho** na página **Otimização de custos**, exibindo detalhes do grupo de entrega selecionado na guia **Utilização de Recursos**.

> **Nota:**
>
> - A configuração da política de Monitoramento, Habilitar Monitoramento de Processos, deve ser definida como "Permitido" para coletar e exibir dados na tabela dos 10 Principais Processos na página Utilização Histórica da Máquina. A política é definida como "Proibido" por padrão. Todos os dados de utilização de recursos são coletados por padrão. Isso pode ser desativado usando a configuração da política Habilitar Monitoramento de Recursos. A tabela abaixo dos gráficos mostra os dados de utilização de recursos por máquina.
> - O IOPS médio mostra as médias diárias. O IOPS de pico é calculado como o maior das médias de IOPS para o intervalo de tempo selecionado. (Uma média de IOPS é a média horária de IOPS coletados durante a hora no VDA).
> - O detalhamento da máquina lista processos com uso médio de CPU ou memória média superior a 1%, o que pode significar que, às vezes, menos de 10 processos são listados.

> **Visualizar falhas de aplicativo:** A guia Falhas de Aplicativo exibe falhas associadas aos aplicativos publicados nos VDAs.

Este recurso requer VDAs **versão 7.15** ou posterior. VDAs de SO de sessão única executando Windows Vista e posterior, e VDAs de SO de várias sessões executando Windows Server 2008 e posterior são suportados. Para obter mais informações, consulte Monitoramento histórico de falhas de aplicativo.

Por padrão, apenas as falhas de aplicativo de VDAs de SO de várias sessões são exibidas. Você pode configurar o monitoramento de falhas de aplicativo usando políticas de Monitoramento. Para obter mais informações, consulte Configurações da política de monitoramento.

Criar relatórios personalizados: A guia Relatórios Personalizados fornece uma interface de usuário para gerar Relatórios Personalizados contendo dados em tempo real e históricos do banco de dados de Monitoramento em formato tabular.

Na lista de consultas de Relatórios Personalizados salvas anteriormente, você pode clicar em **Executar e baixar** para exportar o relatório no formato CSV, clicar em **Copiar OData** para copiar e compartilhar a consulta OData correspondente, ou clicar em **Editar** para editar a consulta. Você pode criar uma consulta de Relatório Personalizado com base em máquinas, conexões, sessões ou instâncias de aplicativo. Especifique condições de filtro com base em campos como máquina, grupo de entrega ou período de tempo. Especifique as colunas extras necessárias em seu Relatório Personalizado. A visualização exibe uma amostra dos dados do relatório. Salvar a consulta de Relatório Personalizado a adiciona à lista de consultas salvas.

Você pode criar uma consulta de Relatório Personalizado com base em uma consulta OData copiada. Para fazer isso, selecione a opção Consulta OData e cole a consulta OData copiada. Você pode salvar a consulta resultante para execução posterior.

> **Nota:**
>
> Os nomes das colunas no relatório de Visualização e Exportação gerado usando consultas OData não são localizados, mas aparecem em inglês.

> Os ícones de bandeira no gráfico indicam eventos ou ações significativas para aquele intervalo de tempo específico. Passe o mouse sobre a bandeira e clique para listar eventos ou ações.

> **Nota:**
>
> - Os dados de logon de conexão HDX™ não são coletados para VDAs anteriores à versão 7. Para VDAs anteriores, os dados do gráfico são exibidos como 0.
> - Os grupos de entrega excluídos no Studio estão disponíveis para seleção nos filtros de Tendências até que os dados relacionados a eles sejam removidos. A seleção de um grupo de entrega excluído exibe gráficos para os dados disponíveis até a retenção. No entanto, as tabelas não mostram dados.

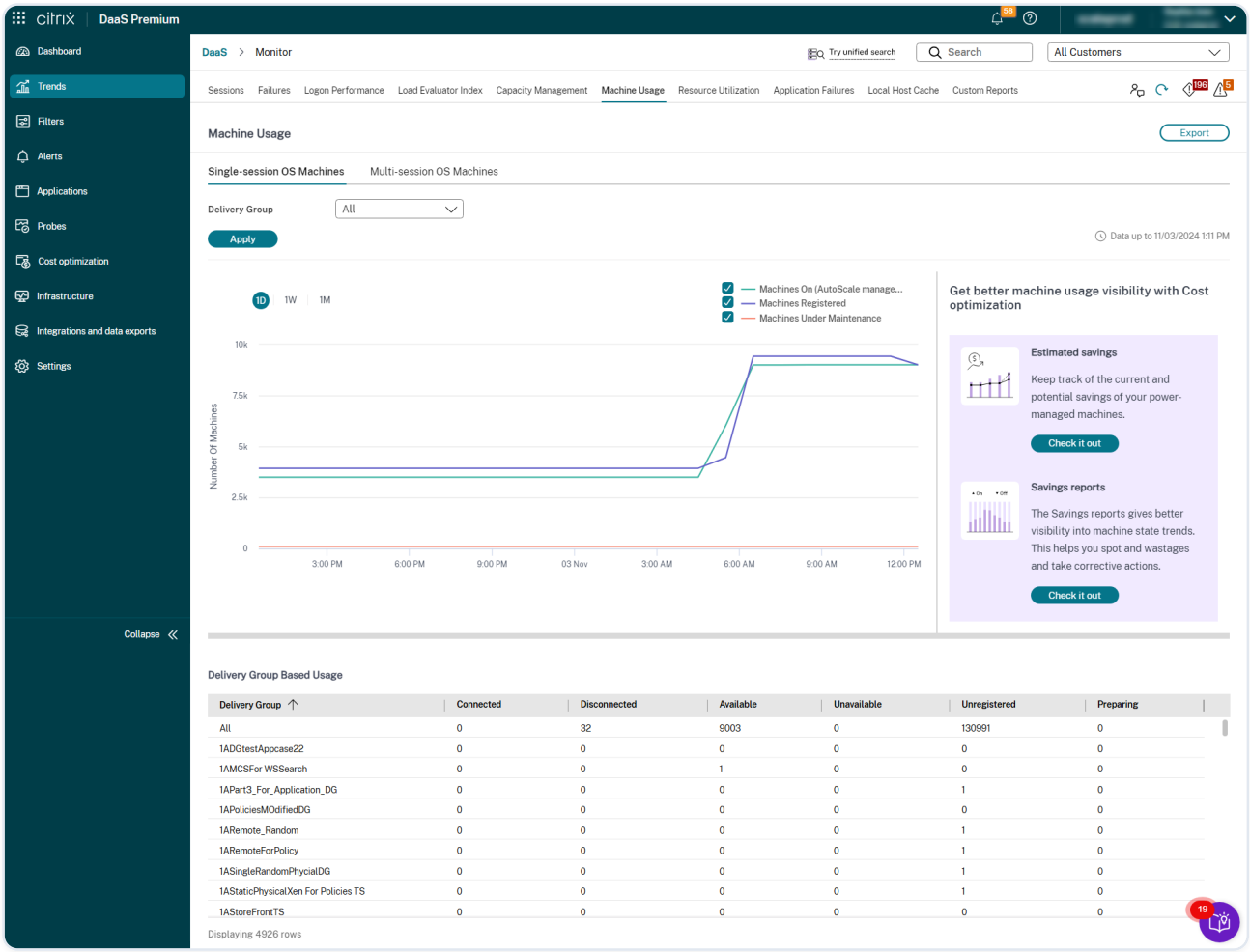
- Mover uma máquina contendo sessões ativas de um grupo de entrega para outro faz com que as tabelas de **Utilização de Recursos e Índice do Avaliador de Carga** do novo grupo de entrega exibam métricas consolidadas dos grupos de entrega antigo e novo.

Monitorar máquinas gerenciadas pelo Autoscale

O Autoscale é um recurso de gerenciamento de energia que permite o gerenciamento proativo de energia de todas as máquinas de SO de sessão única e multissessão registradas em um grupo de entrega. Você pode configurar o Autoscale para um grupo de entrega selecionado na guia **Gerenciar**. Para obter mais informações, consulte Autoscale. Você pode monitorar as principais métricas das máquinas habilitadas para Autoscale no console do **Monitor**.

Uso da Máquina

A página **Monitor** > **Tendências** > **Uso da Máquina** exibe o número total de máquinas de SO de sessão única e multissessão habilitadas para Autoscale que estão ligadas para um grupo de entrega e período de tempo selecionados. Essa métrica indica o uso real das máquinas no grupo de entrega. Na guia **Máquinas de SO de sessão única** ou **Máquinas de SO multissessão**, selecione o grupo de entrega e o período de tempo.

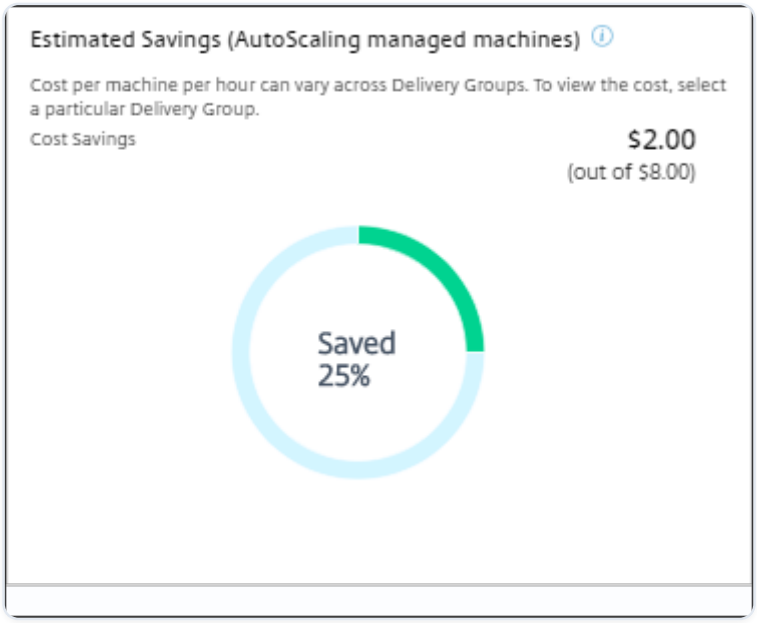


O gráfico plota as seguintes métricas:

- **Máquinas Ligadas** - o número de máquinas habilitadas para Autoscale que estão ligadas
- **Máquinas Registradas** - o número de máquinas de SO de sessão única ou multissessão registradas
- **Máquinas em Manutenção** - o número de máquinas de SO de sessão única ou multissessão com o modo de manutenção ativado

Economia Estimada

A página **Monitor** > **Tendências** > **Uso da Máquina** também exibe a economia de custos estimada alcançada ao habilitar o Autoscale no grupo de entrega selecionado.



A Economia Estimada é calculada como a porcentagem de economia por máquina por hora (em US$) conforme configurado em **Gerenciar** > **Editar Grupo de Entrega** > **Autoscale**. Para obter mais informações sobre como configurar a economia por máquina, consulte Autoscale.

Quando você seleciona todos os grupos de entrega, o valor médio da Economia Estimada em todos os grupos de entrega é exibido. A economia estimada ajuda os administradores a consolidar a infraestrutura existente e planejar a capacidade para obter o máximo de economia e utilização.

Notificações de alerta para máquinas e sessões

O Painel do Monitor exibe notificações de alerta que podem ser detalhadas. Os detalhes do alerta são exibidos na página **Monitor** > **Alertas**.

- Para criar uma política de alerta em um grupo de entrega, vá para **Monitorar** > **Alertas** > **Política de Alertas Citrix** > **Política de Grupo de Entrega**.
- Aqui, você pode definir os seguintes limites de Aviso e Crítico:
  - Máquinas com Falha (SO de sessão única) e Máquinas com Falha (SO de múltiplas sessões),
  - Sessões Conectadas de Pico, Sessões Desconectadas de Pico e Sessões Concorrentes Totais de Pico no grupo de entrega.
- Os alertas são gerados quando a métrica correspondente no grupo de entrega atinge o limite.

Para mais detalhes sobre as condições da política de alerta e a criação de novas políticas de alerta, consulte Alertas e notificações.

Status da máquina

- **Monitorar** > **Filtros** > **Máquinas** exibe o estado de energia de todas as máquinas em formato tabular. Você pode filtrar por um grupo de entrega específico.
- **Monitorar** > **Filtros** > **Sessões** exibe o filtro pelo nome da Máquina para ver as sessões associadas e seu status em tempo real.
- Em **Monitorar** > **Tendências** > **Sessões**, selecione seu grupo de entrega e período para ver a tendência das sessões e suas métricas associadas.

Para mais informações, consulte Filtrar dados para solucionar falhas.

Tendências de Avaliação de Carga

A página **Monitorar** > **Tendências** > **Índice do Avaliador de Carga** exibe um gráfico com informações detalhadas sobre a carga distribuída entre as máquinas de SO de múltiplas sessões. As opções de filtro para este gráfico incluem o grupo de entrega ou máquina de SO de múltiplas sessões em um grupo de entrega, máquina de SO de múltiplas sessões (disponível apenas se a máquina de SO de múltiplas sessões em um grupo de entrega foi selecionada) e intervalo. O Índice do Avaliador de Carga é exibido como porcentagens de CPU Total, Memória, Disco ou Sessões e é mostrado em comparação com o número de usuários conectados no último intervalo.

Solucionar problemas de implantações

Como administrador de help desk, você pode pesquisar o usuário que está relatando um problema. E, então, exibir os detalhes das sessões ou aplicativos associados a esse usuário.

Da mesma forma, você pode pesquisar máquinas ou endpoints onde os problemas são relatados. Os problemas podem ser rapidamente resolvidos monitorando as métricas relevantes e realizando as ações adequadas.

As seguintes ações estão disponíveis:

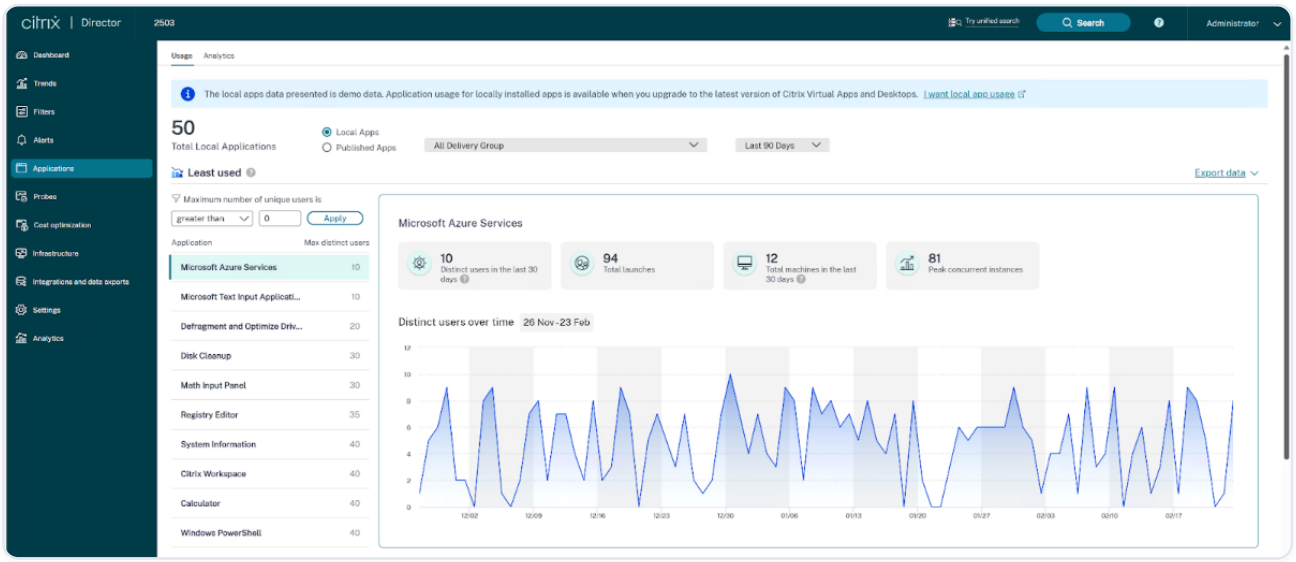
- encerrar um aplicativo ou processo que não responde
- sombrear operações na máquina do usuário
- fazer logoff de uma sessão que não responde
- reiniciar a máquina
- colocar uma máquina em modo de manutenção

- redefinir o perfil do usuário

Solucionar problemas de aplicativos

Análise de Aplicativos

A exibição de **Aplicativos** exibe análises baseadas em aplicativos em uma única exibição consolidada para ajudar a analisar e gerenciar o desempenho dos aplicativos de forma eficiente. Você pode obter informações valiosas sobre a integridade e o uso de todos os aplicativos publicados no site. A exibição padrão ajuda a identificar os principais aplicativos em execução. Este recurso requer VDAs Versão 7.15 ou posterior.



A coluna **Instâncias** exibe o uso dos aplicativos. Ela indica o número de instâncias de aplicativos atualmente em execução (instâncias conectadas e desconectadas). Para solucionar problemas adicionais, clique no campo **Instâncias** para ver a página de filtros correspondente de **Instâncias de Aplicativos**. Aqui, você pode selecionar instâncias de aplicativos para fazer logoff ou desconectar.

> **Nota:**
>
> Para administradores de escopo personalizado, o Monitor não exibe instâncias de aplicativos criadas em grupos de aplicativos. Para visualizar todas as instâncias de aplicativos, você deve ser um administrador completo. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX256001.

> Monitore a integridade dos aplicativos publicados em seu site com as colunas **Falhas de Aplicativo** e **Erros de Aplicativo**. Essas colunas exibem o número agregado de falhas e erros que ocorreram ao iniciar o aplicativo correspondente na última hora. Clique no campo **Falhas de Aplicativo** ou **Erros de Aplicativo** para ver os detalhes da falha na página **Tendências** \> **Falhas de Aplicativo** correspondente ao aplicativo selecionado.

As configurações da política de falha de aplicativo governam a disponibilidade e a exibição de falhas e erros. Para obter mais informações sobre as políticas e como modificá-las, consulte Políticas para monitoramento de falhas de aplicativo nas configurações da política de monitoramento.

Monitoramento de aplicativos em tempo real

Você pode solucionar problemas de aplicativos e sessões usando a métrica de tempo ocioso para identificar instâncias que estão ociosas além de um limite de tempo específico.

Casos de uso típicos para solução de problemas baseada em aplicativos são no setor de saúde, onde os funcionários compartilham licenças de aplicativos. Lá, você deve encerrar sessões ociosas e instâncias de aplicativos para limpar o ambiente Citrix Virtual Apps and Desktops™, reconfigurar servidores com baixo desempenho ou manter e atualizar aplicativos.

A página de filtro **Instâncias de Aplicativos** lista todas as instâncias de aplicativos em VDAs de SO de múltiplas sessões e de sessão única. As medições de tempo ocioso associadas são exibidas para instâncias de aplicativos em VDAs de SO de múltiplas sessões que estiveram ociosas por pelo menos 10 minutos.

> **Nota:**

> As métricas de Instâncias de Aplicativos estão disponíveis em sites de todas as edições de licença.

> Use esta informação para identificar as instâncias de aplicativo que estão ociosas além de um período de tempo específico e desconectá-las ou encerrar a sessão conforme apropriado. Para fazer isso, selecione **Filtros \> Instâncias de Aplicativo** e selecione um filtro pré-salvo ou escolha **Todas as Instâncias de Aplicativo** e crie seu próprio filtro.

Filtro de instâncias de aplicativo(/en-us/citrix-daas/media/dir-troubleshoot-applications.png)

Um exemplo de filtro seria o seguinte. Como critérios de **Filtrar por**, escolha **Nome Publicado** (do aplicativo) e **Tempo Ocioso**. Em seguida, defina **Tempo Ocioso** como **maior ou igual a** um limite de tempo específico e salve o filtro para reutilização. Na lista filtrada, selecione as instâncias de aplicativo. Selecione a opção para enviar mensagens ou, no menu suspenso **Controle de Sessão**, escolha **Encerrar Sessão** ou **Desconectar** para finalizar as instâncias.

> **Nota:**
>
> Encerrar a sessão ou desconectar uma instância de aplicativo encerra a sessão ou desconecta a sessão atual, finalizando assim todas as instâncias de aplicativo que pertencem à mesma sessão.
>
> Você pode identificar sessões ociosas na página de filtro **Sessões** usando o estado da sessão e a métrica de tempo ocioso da sessão. Classifique pela coluna **Tempo Ocioso** ou defina um filtro para identificar sessões que estão ociosas além de um limite de tempo específico. O tempo ocioso é listado para sessões em VDAs de SO multi-sessão que estiveram ociosas por pelo menos 10 minutos.

Filtro de sessões(/en-us/citrix-daas/media/dir-troubleshoot-sessions.png)

O **Tempo ocioso** é exibido como **N/A** quando a sessão ou instância de aplicativo

- não esteve ociosa por mais de 10 minutos,
- é iniciada em um VDA de SO de sessão única, ou
- é iniciada em um VDA executando a Versão 7.12 ou anterior.

Monitoramento histórico de falhas de aplicativo

A guia **Tendências** -\> **Falhas de Aplicativo** exibe as falhas associadas aos aplicativos publicados nos VDAs.

Para obter mais informações sobre a disponibilidade das tendências de falha de aplicativo, consulte o artigo Granularidade e retenção de dados. As falhas de aplicativo que são registradas no Visualizador de Eventos com a origem "Erros de Aplicativo" são monitoradas. Clique em **Exportar** para gerar relatórios nos formatos CSV, Excel ou PDF

Tendência de falha de aplicativo(/en-us/citrix-daas/media/dir_application_faults.png)

As falhas são exibidas como **Falhas de Aplicativo** ou **Erros de Aplicativo** com base em sua gravidade. A guia Falhas de Aplicativo exibe falhas associadas à perda de funcionalidade ou dados. Erros de Aplicativo indicam problemas que não são imediatamente relevantes; eles significam condições que podem causar problemas futuros.

Você pode filtrar as falhas com base em **Nome do Aplicativo Publicado**, **Nome do Processo** ou **Grupo de Entrega** e **Período de Tempo**. A tabela exibe o código da falha ou erro e uma breve descrição da falha. A descrição detalhada da falha é exibida como uma dica de ferramenta.

> **Nota:**
>
> O nome do Aplicativo Publicado é exibido como “Desconhecido” quando o nome do aplicativo correspondente não pode ser derivado. Isso geralmente ocorre quando um aplicativo iniciado falha em uma sessão de desktop ou quando falha devido a uma exceção não tratada causada por um executável dependente.

> Por padrão, apenas as falhas de aplicativos hospedados em VDAs de SO multi-sessão são monitoradas. Você pode modificar as configurações de monitoramento por meio das Políticas de Grupo de Monitoramento: Habilitar monitoramento de falhas de aplicativo, Habilitar monitoramento de falhas de aplicativo em VDAs de SO de sessão única e Lista de aplicativos excluídos do monitoramento de falhas. Para mais informações, consulte Políticas para monitoramento de falhas de aplicativo em Configurações de política de monitoramento.

Sondagem de aplicativos

A sondagem de aplicativos automatiza o processo de verificação da integridade dos aplicativos Citrix Virtual Apps publicados em um site. Os resultados da sondagem de aplicativos estão disponíveis no console **Monitor** do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™). O Citrix Probe Agent oferece suporte a sites hospedados no Citrix Cloud Japan e nos Planos de Controle do Citrix Cloud Government.

Certifique-se de que as máquinas de endpoint que executam agentes de sondagem sejam máquinas Windows com Citrix Receiver para Windows Versão 4.8 ou posterior, ou Citrix Workspace app para Windows (anteriormente Citrix Receiver para Windows) Versão 1808 ou posterior. O Workspace app para Unified Windows Platform (UWP) não é compatível.

Requisitos:

- As máquinas de endpoint que executam agentes de sondagem são máquinas Windows com Citrix Receiver para Windows Versão 4.8 ou posterior, ou Citrix Workspace app para Windows (anteriormente Citrix Receiver para Windows) Versão 1906 ou posterior. O Workspace app para Unified Windows Platform (UWP) não é compatível.
- O Citrix Probe Agent oferece suporte à autenticação padrão baseada em formulário, conforme suportado pelo Citrix® StoreFront Cloud. O Citrix Probe Agent não oferece suporte a outros métodos de autenticação, como Single Sign-On (SSO) ou Multi Factor Authentication (MFA). Da mesma forma, o Citrix Probe Agent funciona apenas quando não há um servidor proxy ou balanceador de carga como o Citrix Gateway ou o Citrix ADC implantado.
- Certifique-se de que o Microsoft .NET Framework versão 4.7.2 ou posterior esteja instalado na máquina de endpoint onde você deseja instalar o Probe Agent.
- Para usar o agente de sondagem no Plano de Controle do Citrix Cloud Japan, defina o valor do registro no caminho "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" como 2. Para usar o agente de sondagem no Plano de Controle do Citrix Cloud Government, defina o valor do registro no caminho "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" como 3.

As contas de usuário/permissões necessárias para executar a Sondagem de Aplicativos são as seguintes:

- Um usuário exclusivo para sondar em cada máquina de endpoint. O usuário não precisa ser um administrador; as sondagens podem ser executadas em um contexto não administrativo.
- Contas de usuário com permissões de administrador do Windows para instalar e configurar o Citrix Probe Agent nas máquinas de endpoint
- Uma conta de usuário de administrador completo com as seguintes permissões. A reutilização de contas de usuário existentes para sondagem de aplicativos pode desconectar os usuários de suas sessões ativas.
    - Permissões de grupo de entrega:
        - Somente leitura
    - Permissões de Director:
        - Criar\Editar\Remover Configurações de Sondagem
        - Página de Visualização de Configurações

- Página de Visualização de Tendências

Configurar Sondagem de Aplicativos

Configure suas sondagens de aplicativos para serem executadas durante horários de pico em várias regiões geográficas. Os resultados abrangentes da sondagem podem ajudar a solucionar problemas relacionados aos aplicativos, máquina de hospedagem ou conexão antes que os usuários os experimentem.

O Citrix Probe Agent versão 2103 suporta agregação de sites. Aplicativos e desktops podem ser enumerados e iniciados a partir de sites agregados. Ao configurar o agente de sondagem, selecione a opção **Agregação de Sites do Workspace (StoreFront) Habilitada** para permitir a enumeração de aplicativos e desktops de sites agregados. As seguintes combinações de sites são suportadas:

- Vários sites locais com uma URL de loja.
- Sites locais e na nuvem com uma URL de loja local ou uma URL de loja na nuvem.
- Vários sites na nuvem com uma URL de loja.

> **Nota:**
>
> Você deve criar administradores ou usuários separados para configurar sondagens que tenham acesso a apenas um site.

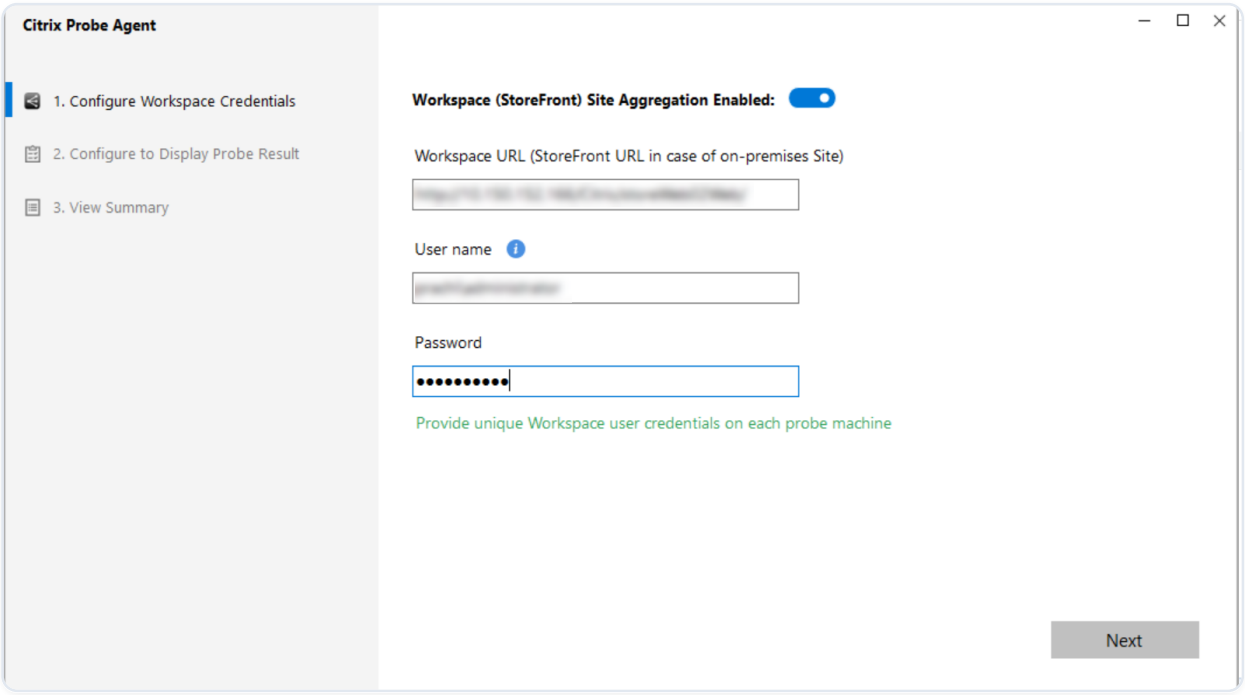
ETAPA 1: INSTALAR E CONFIGURAR O CITRIX PROBE AGENT

O Citrix Probe Agent é um executável do Windows que simula o lançamento real de aplicativos pelo usuário através do aplicativo Citrix Workspace. Ele testa os lançamentos de aplicativos conforme configurado no Monitor e reporta os resultados de volta ao Monitor.

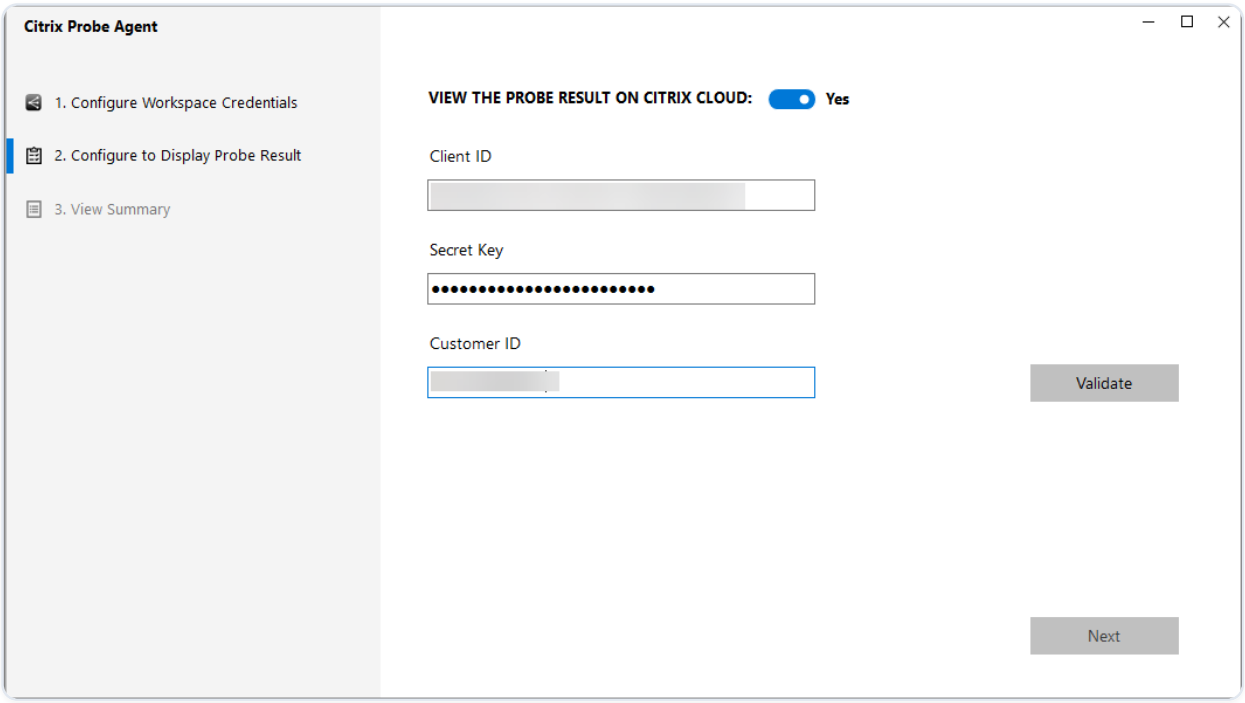
1. Identifique as máquinas de endpoint de onde você deseja executar a sondagem de aplicativos.
2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina de endpoint. Baixe o executável do Citrix Probe Agent disponível em `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/edition-software/premium-2411.html>`
3. Inicie o agente e insira as credenciais para o usuário com o qual a sonda deve fazer login. Configure um usuário exclusivo em cada máquina de endpoint. As credenciais são criptografadas e armazenadas com segurança.

Observações:

- Para acessar o site a ser sondado de fora da rede, digite o URL de login do Citrix Gateway no campo **URL da loja**. O Citrix Gateway roteia automaticamente a solicitação para o URL da loja do site correspondente.
- Use NetBIOS como nome de domínio no campo de nome de usuário. Por exemplo, NetBIOS/nome_de_usuário.
- A sondagem de aplicativos suporta o serviço Citrix Content Collaboration™ usando autenticação (somente AD).



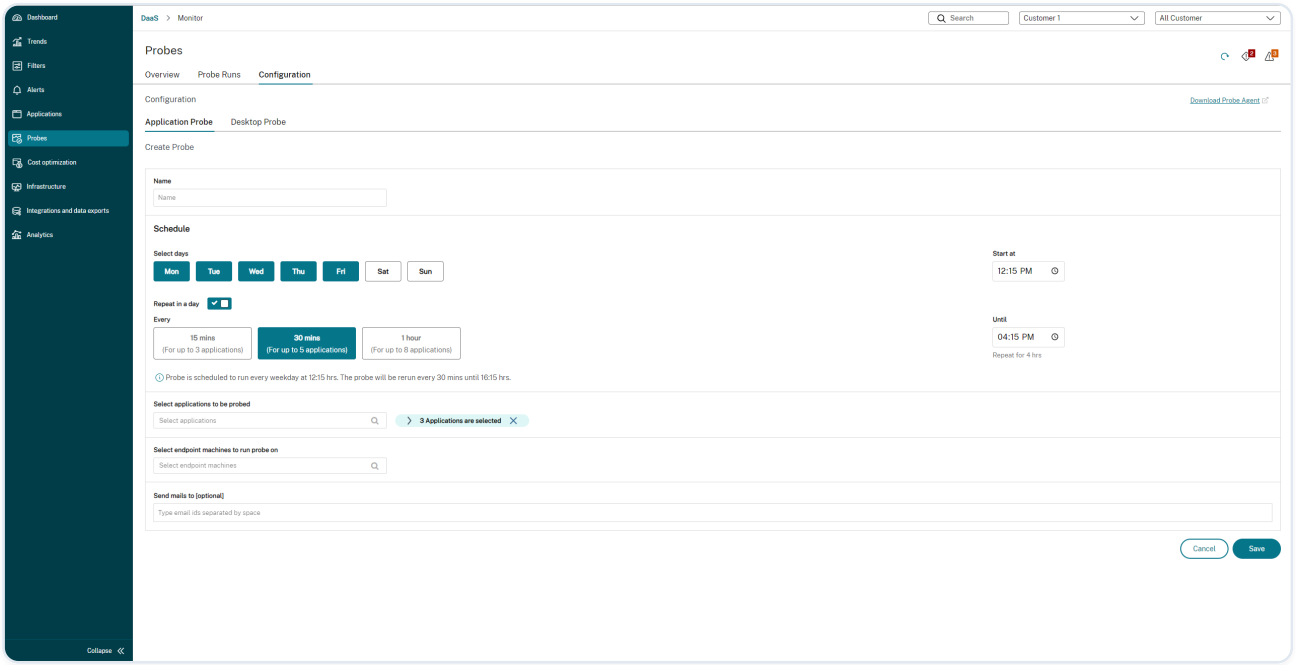
4. Na guia **Configurar para Exibir Resultado da Sonda**, insira as credenciais para acessar o Citrix DaaS. Você pode encontrar o Nome do Cliente ou ID do Cliente, ID do Cliente e Chave Secreta na página Acesso à API no console do Citrix Cloud™.



ETAPA 2: CONFIGURAR A SONDAGEM DE APLICATIVOS NA GUIA MONITOR

1. No Citrix DaaS, vá para **Configuração** \> **Configuração da Sonda** \> **Sonda de Aplicativo** e clique em **Criar Sonda**:
2. Na página **Criar Sonda**, insira o nome da sonda.
3. Selecione o agendamento:
    a. Escolha os dias da semana em que deseja que a sonda seja executada.
    b. Insira a hora de início em que deseja que a sonda seja executada.
    c. Além disso, você pode escolher a opção **Repetir em um dia**. Insira a hora de término e o intervalo em que deseja que a sonda se repita dentro de um dia. Por exemplo, a configuração abaixo ajuda a executar sondas de aplicativos das 12:08 horas até as 16:34 horas, repetindo a cada 30 minutos todas as segundas, quartas, quintas e domingos.
4. Selecione o número recomendado de aplicativos a serem sondados dependendo do intervalo.
5. Selecione as máquinas de endpoint nas quais a sondagem deve ser executada.
6. Insira os endereços de e-mail para os quais os resultados da sondagem de falha são enviados e clique em **Salvar**.

Nesta configuração, as sessões do aplicativo são iniciadas às 12:08 horas, 12:38 horas, 13:08 horas e assim por diante até as 16:08 horas todas as segundas, quartas, quintas e domingos.



Nota:

- Configure seu servidor de e-mail em **Alertas** > **Configuração do Servidor de E-mail**.
- Após a configuração no console do **Monitor**, o agente executa as sondagens configuradas a partir da próxima hora.
- As sondagens que foram configuradas antes da introdução da opção **Repetir em um dia** continuam a ser executadas no horário programado. Elas têm a opção **Repetir em um dia** desativada por padrão.

ETAPA 3: EXECUÇÃO DA SONDAGEM

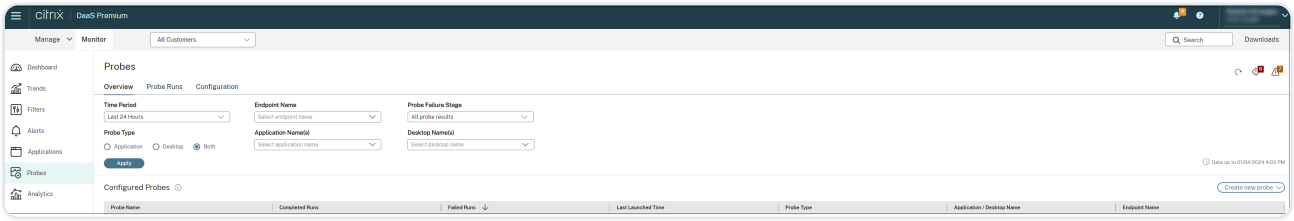
O agente executa a sondagem de aplicativos de acordo com a configuração de sondagem que ele busca do Monitor a cada hora. Ele inicia os aplicativos selecionados serialmente usando o Workspace. O agente reporta os resultados de volta ao Monitor através do banco de dados do Monitor. As falhas são reportadas em cinco estágios específicos:

- **Acessibilidade do Workspace** - a URL da loja configurada não está acessível.
- **Autenticação do Workspace** - as credenciais configuradas são inválidas.
- **Enumeração do Workspace** - A lista de aplicativos enumerados não contém o aplicativo a ser sondado.

- **Download do ICA®** - o arquivo ICA não está disponível.
- **Inicialização do aplicativo** – o aplicativo não pode ser iniciado.

ETAPA 4: VISUALIZAR RESULTADOS DA SONDAGEM

Você pode visualizar os resultados mais recentes da sondagem na página Citrix DaaS™ > **Aplicativos**.



Para solucionar problemas adicionais, clique no link do resultado da sondagem para ver mais detalhes na página **Tendências** \> **Resultados da Sondagem de Aplicativos**.

Os dados consolidados dos resultados da sondagem estão disponíveis para os períodos das últimas 24 horas ou últimos 7 dias nesta página. Você pode ver o estágio em que a sondagem falhou. Você pode filtrar a tabela para um aplicativo específico, estágio de falha da sondagem ou máquina de endpoint.

Sondagem de desktop

A sondagem de desktop automatiza o processo de verificação da integridade dos Citrix Virtual Desktops™ que são publicados em um site. Os resultados da sondagem de desktop estão disponíveis no Monitor. O Citrix Probe Agent agora oferece suporte a sites hospedados no Citrix Cloud Japan e nos Planos de Controle do Citrix Cloud Government.

Na página Configuração do Monitor, configure os desktops a serem sondados, as máquinas de endpoint para executar a sondagem e o tempo da sondagem. O agente testa o lançamento dos desktops selecionados usando o aplicativo Citrix Workspace e relata os resultados de volta ao Monitor. Os resultados da sondagem são exibidos na interface do usuário do Monitor – os dados das últimas 24 horas na página Aplicativos e os dados históricos da sondagem na página **Tendências > Resultados da Sondagem > Resultados da Sondagem de Desktop**.

Aqui, você pode ver o estágio em que a falha da sondagem ocorreu - Acessibilidade do Workspace, Autenticação do Workspace, Enumeração do Workspace, download do ICA® ou lançamento do Desktop. O relatório de falha é enviado para os endereços de e-mail configurados.

Você pode agendar suas sondagens de desktop para serem executadas durante o horário de pico em várias regiões geográficas. Os resultados abrangentes podem ajudar a solucionar

proativamente problemas relacionados a desktops provisionados, máquinas de hospedagem ou conexões antes que os usuários os experimentem.

Este recurso requer o Probe Agent 1903 ou posterior.

Requisitos:

- As máquinas de endpoint que executam agentes de sondagem são máquinas Windows com Citrix Receiver para Windows Versão 4.8 ou posterior, ou Citrix Workspace app para Windows (anteriormente Citrix Receiver para Windows) Versão 1906 ou posterior. O aplicativo Workspace para Unified Windows Platform (UWP) não é compatível.
- O Citrix Probe Agent oferece suporte à autenticação padrão baseada em formulário, conforme suportado pelo StoreFront e StoreFront Cloud. O Citrix Probe Agent não oferece suporte a outros métodos de autenticação, como Single Sign-On (SSO) ou Multi Factor Authentication (MFA). Da mesma forma, o Citrix Probe Agent funciona apenas quando não há um servidor proxy ou balanceador de carga como o Citrix Gateway ou o Citrix ADC implantado.
- Certifique-se de que o Microsoft .NET Framework versão 4.7.2 ou posterior esteja instalado na máquina de endpoint onde você deseja instalar o Probe Agent.
- Para usar o agente de sondagem no Plano de Controle do Citrix Cloud Japan, defina o valor do registro no caminho, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" como 2. Para usar o agente de sondagem no Plano de Controle do Citrix Cloud Government, defina o valor do registro no caminho, "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" como 3.

Contas de usuário ou permissões necessárias para executar a sondagem de desktop:

- Um usuário exclusivo para sondar em cada máquina de endpoint. O usuário não precisa ser um administrador; as sondagens podem ser executadas em um contexto não administrativo.
- Contas de usuário com permissões de administrador do Windows para instalar e configurar o Citrix Probe Agent nas máquinas de endpoint
- Uma conta de usuário de administrador completo ou uma função personalizada com as seguintes permissões. Reutilizar contas de usuário normais para sondagem de desktop pode desconectar os usuários das sessões ativas.
    - Permissões do grupo de entrega:
        - Somente leitura

- Permissões do Monitor:
  - Criar, Editar, Remover Configuração do Servidor de E-mail de Alerta - se o servidor de e-mail ainda não estiver configurado
  - Criar, Editar, Remover Configurações de Sondagem
  - Visualizar página de Configurações
  - Visualizar página de Tendências

Configurar sondagem de desktop

Você pode agendar suas sondagens de desktop para serem executadas durante horários de pico em várias regiões geográficas. Os resultados abrangentes da sondagem podem ajudar a solucionar problemas relacionados aos desktops, máquina de hospedagem ou conexão antes que os usuários os experimentem.

O Citrix Probe Agent versão 2103 suporta agregação de sites. Aplicativos e desktops podem ser enumerados e iniciados a partir de sites agregados. Ao configurar o agente de sondagem, selecione a opção **Agregação de Sites do Workspace (StoreFront) Ativada** para permitir a enumeração de aplicativos e desktops de sites agregados. As seguintes combinações de sites são suportadas:

- Vários sites locais com uma URL de loja.
- Sites locais e na nuvem com uma URL de loja local ou uma URL de loja na nuvem.
- Vários sites na nuvem com uma URL de loja.

> **Nota:**
>
> Você deve criar administradores ou usuários separados para configurar sondagens que tenham acesso a apenas um site.

PASSO 1: INSTALAR E CONFIGURAR O CITRIX PROBE AGENT

O Citrix Probe Agent é um executável do Windows que simula o lançamento real da área de trabalho pelo usuário através do Workspace. Ele testa os lançamentos da área de trabalho conforme configurado no Monitor e reporta os resultados de volta ao Monitor.

1. Identifique as máquinas de endpoint de onde você deseja executar a sondagem de área de trabalho.

2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina de endpoint. Baixe o executável do Citrix Probe Agent disponível em `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/edition-software/premium-2411.html>`
3. Inicie o agente e configure suas credenciais do Workspace Receiver for Web. Configure um usuário Workspace exclusivo em cada máquina de endpoint. As credenciais são criptografadas e armazenadas com segurança.

   > **Observações:**

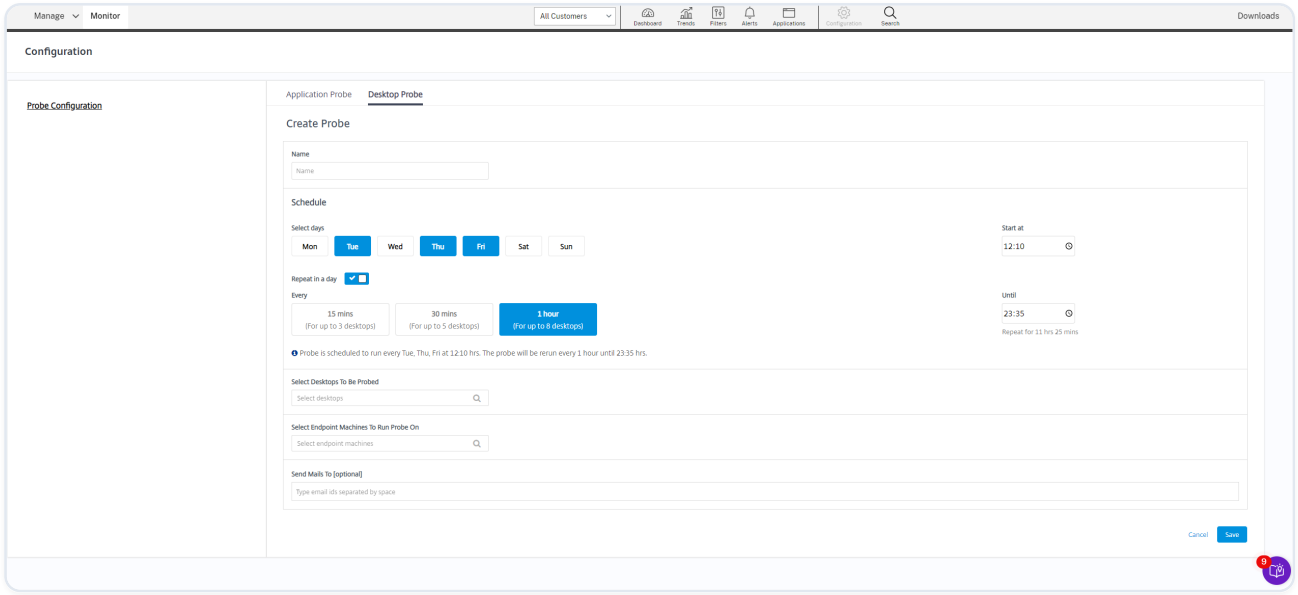
   - Para acessar o site a ser sondado de fora da rede, digite a URL da página de login do Citrix Gateway no campo de URL da loja. O Citrix Gateway roteia automaticamente a solicitação para a URL da loja do site correspondente. Este recurso está disponível para o Citrix Gateway versão 12.1 ou posterior.
   - Use NetBIOS como o nome de domínio no campo de nome de usuário. Por exemplo, NetBIOS/nome_de_usuário.
   - A sondagem de área de trabalho suporta o serviço Citrix Content Collaboration™ usando autenticação do Workspace (somente AD).
   - Você deve habilitar o Logon Interativo para o usuário exclusivo do StoreFront configurado.
4. Na guia **Configurar para Exibir Resultado da Sondagem**, insira suas credenciais do Monitor. Você pode encontrar o Nome do Cliente ou ID do Cliente, ID do Cliente e Chave Secreta na página Acesso à API no console do Citrix Cloud™.

PASSO 2: CONFIGURAR A SONDAGEM DE ÁREA DE TRABALHO NO MONITOR

1. No Citrix DaaS, vá para **Configuração** \> **Configuração da Sondagem** \> **Sondagem de Aplicativo** e clique em **Criar Sondagem**.
2. Na página **Criar Sondagem**, insira o nome da sondagem.
3. Selecione o agendamento:
   a. Escolha os dias da semana em que você deseja que a sondagem seja executada.
   b. Insira a hora de início em que você deseja que a sondagem seja executada.
   c. Além disso, você pode escolher a opção **Repetir em um dia**. Insira a hora de término e o intervalo em que você deseja que a sondagem se repita dentro de um dia. Por exemplo, a configuração abaixo ajuda a executar sondagens de desktop das 12:10 horas até as 23:35 horas, repetindo a cada hora, todas as terças, quintas e sextas-feiras.

4. Selecione o número recomendado de desktops a serem sondados, dependendo do intervalo.
5. Selecione as máquinas de endpoint nas quais a sondagem deve ser executada.
6. Insira os endereços de e-mail para os quais os resultados da sondagem de falha são enviados e clique em **Salvar**.

Nesta configuração, as sessões de desktop são iniciadas às 12:10 horas, 13:10 horas, 14:10 horas e assim por diante até as 23:10 horas, todas as terças, quintas e sextas-feiras.



Nota:

- Configure seu servidor de e-mail em **Alertas** > **Configuração do Servidor de E-mail**.
- Após a conclusão da configuração da sondagem de desktop, o agente executa as sondagens configuradas a partir da próxima hora.
- As sondagens que foram configuradas antes da introdução da opção **Repetir em um dia** continuam a ser executadas no horário programado. Elas têm a opção **Repetir em um dia** desativada por padrão.

ETAPA 3: EXECUÇÃO DA SONDAGEM

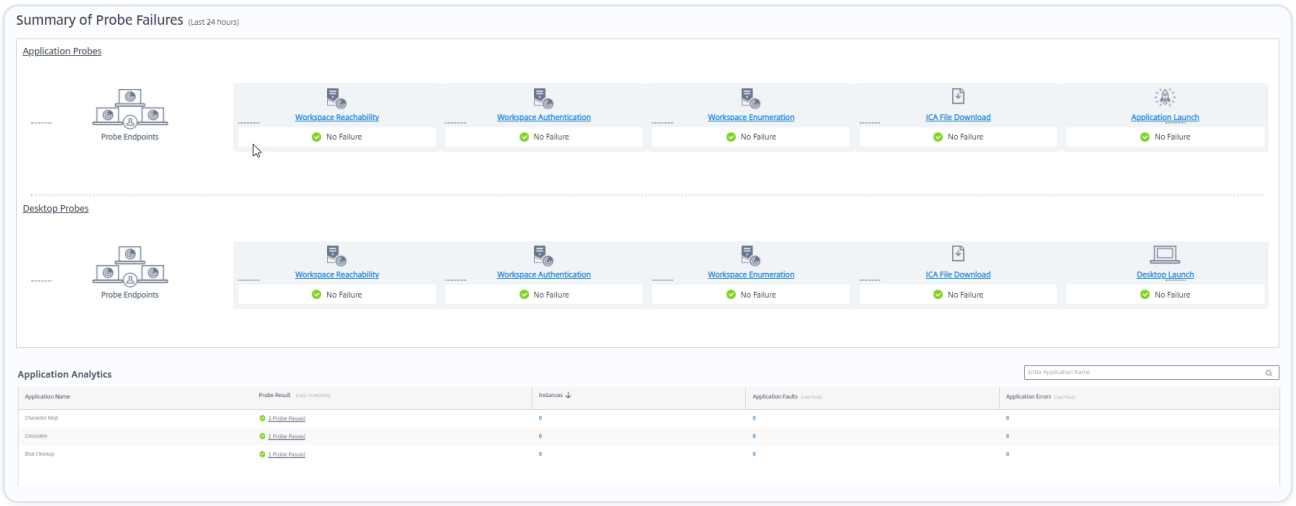
O agente executa a sondagem de desktop de acordo com a configuração da sondagem que ele busca do Monitor periodicamente. Ele inicia os desktops selecionados serialmente usando o Workspace. O agente reporta os resultados de volta ao Monitor através do banco de dados do Monitor. As falhas são relatadas em cinco estágios específicos:

- **Acessibilidade do Workspace** - a URL da loja configurada não está acessível.

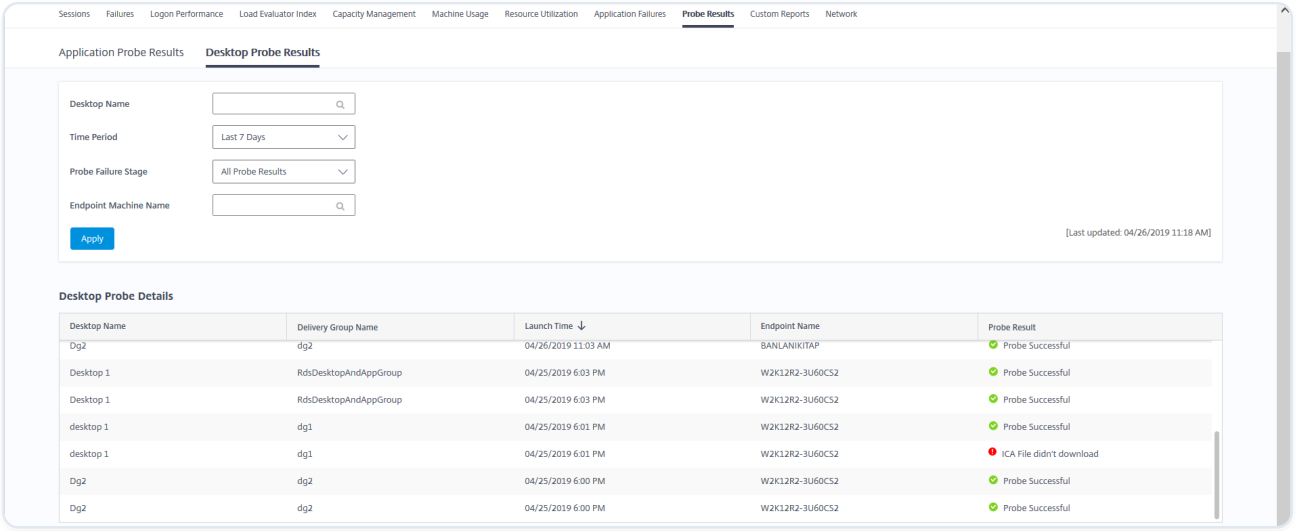
- **Autenticação do Workspace** - as credenciais configuradas são inválidas.
- **Enumeração do Workspace** - A lista de desktops enumerados não contém o desktop a ser sondado.
- **Download do ICA** - o arquivo ICA não está disponível.
- **Inicialização do desktop** – o desktop não pode ser inicializado.

ETAPA 4: VISUALIZAR RESULTADOS DA SONDAGEM

Você pode visualizar os resultados mais recentes da sondagem na página **Desktops**.



Para solucionar problemas adicionais, clique no link do resultado da sondagem para ver mais detalhes na página **Tendências** >**Resultados da Sondagem** > **Resultados da Sondagem de Desktop**.



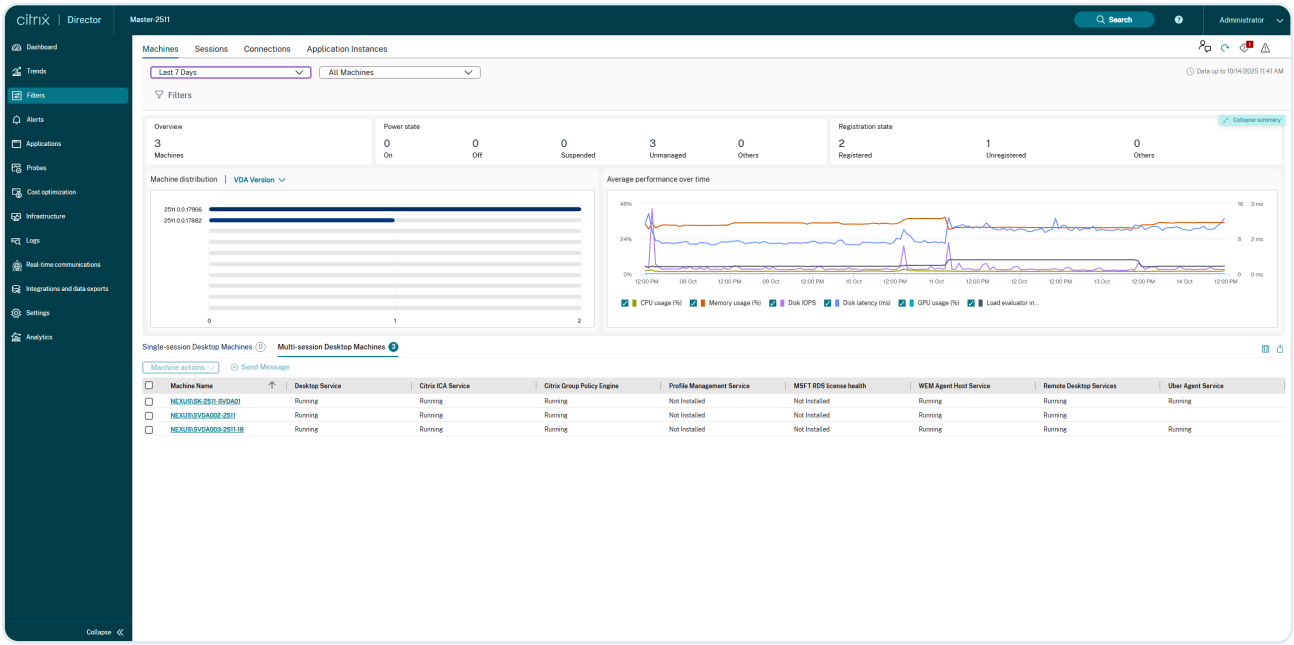
Os dados consolidados dos resultados da sondagem estão disponíveis para os períodos das últimas 24 horas ou últimos 7 dias nesta página. Você pode ver o estágio em que a sondagem falhou. Você pode filtrar a tabela por um desktop específico, estágio de falha da sondagem ou máquina de endpoint.

Monitoramento da saúde da máquina

1. Introdução: O que há de novo?

Para fornecer informações mais detalhadas sobre a saúde e o desempenho das máquinas Virtual Delivery Agent (VDA), introduzimos várias melhorias importantes:

- **Novas Visualizações:**
  a. Um Painel de Resumo foi adicionado com três categorias: **Visão Geral, Estado de Energia** e **Estado de Registro**.
  b. Dois novos gráficos, **Distribuição da máquina** e **Desempenho médio ao longo do tempo**, foram adicionados para fornecer uma visão gráfica imediata do status da máquina e das tendências históricas.
- **Dados Tabulares Aprimorados:** As tabelas de Máquinas de **Desktop de Sessão Única** e **Multissessão** agora incluem colunas de status detalhadas para serviços VDA críticos, ajudando a identificar rapidamente a causa raiz dos problemas de saúde da máquina.
- **Novo Filtro de Intervalo de Tempo:** Dois novos filtros de intervalo de tempo - Últimas 2 Horas e Últimos 7 Dias - foram adicionados para fornecer suporte a tendências históricas.



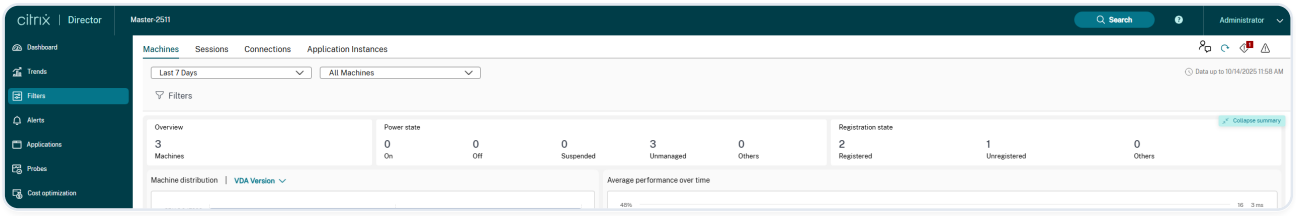
2. Compreendendo as Novas Visualizações

2.1. Painel de Resumo

- **Visão Geral:** Exibe o número total de VDAs (Máquinas) associados.

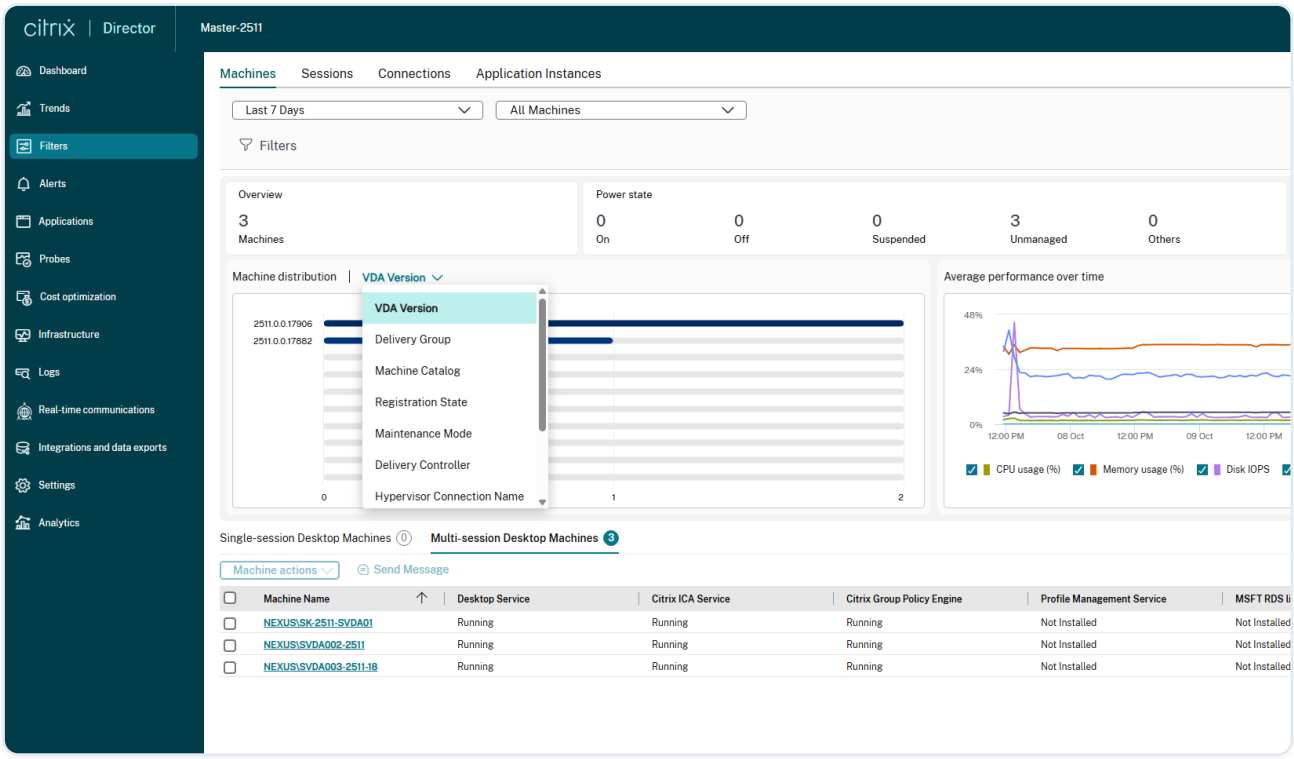
- **Estado de Energia:** Exibe o número de máquinas com base em seus estados de energia - Ligado, Desligado, Suspenso, Não Gerenciado e Outros.
- **Estado de Registro:** Exibe o número de máquinas com base em seus estados de registro - Registrado, Não Registrado e Outros.

Este resumo é recolhível e ajuda os administradores a tomar as ações necessárias com base na segregação acima, como ligar máquinas que estão no estado Desligado ou identificar quais máquinas estão em estados Não Registrados.

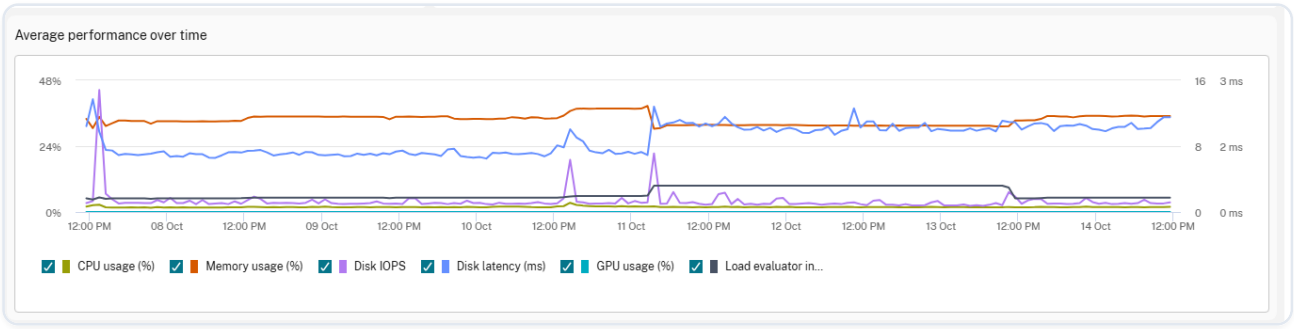


2.2. Distribuição de Máquinas

- **Objetivo:** Este gráfico de barras fornece uma análise visual rápida das máquinas VDA incluídas no conjunto de filtros atual. O filtro padrão é definido como Versão do VDA. No entanto, o usuário pode filtrar usando Grupo de Entrega, Catálogo de Máquinas, Estado de Registro, Modo de Manutenção, Controlador de Entrega, Nome da Conexão do Hypervisor, Tipo de Falha, Motivo da Falha e Estado de Energia.
- **Utilidade:** Isso permite que o administrador obtenha uma visão geral dos VDAs com base nos critérios de filtro. Por exemplo, a Distribuição de Máquinas por Versão do VDA ajuda os administradores a identificar rapidamente se uma parte significativa dos VDAs está executando uma versão mais antiga ou não padrão do VDA, o que pode ser um pré-requisito para solução de problemas ou planejamento de atualização.



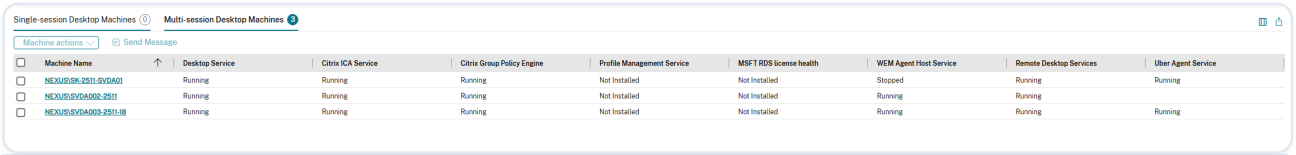
2.3. Desempenho Médio ao Longo do Tempo



- **Objetivo:** Este gráfico de série temporal rastreia as principais métricas de desempenho ao longo do intervalo de tempo selecionado (por exemplo, Últimas 24 Horas).
- **Métricas Principais Monitoradas:**
  - **Uso da CPU (%):** A porcentagem média de CPU sendo utilizada.
  - **Uso da memória (%):** A porcentagem média de RAM sendo utilizada.
  - **IOPS de Disco:** O número médio de Operações de Entrada/Saída por Segundo.
  - **Latência do disco (ms):** O atraso médio (em milissegundos) para solicitações de E/S de disco.
  - **Uso da GPU (%):** A porcentagem média de GPU sendo utilizada (se aplicável).
  - **Avaliador de Carga (%):** A porcentagem do índice de carga calculada na máquina VDA.
- **Utilidade:** Permite a análise de tendências históricas, ajudando a identificar degradação de desempenho, contenção de recursos e quando ocorrem cargas de pico.

3. Dados Tabulares Aprimorados

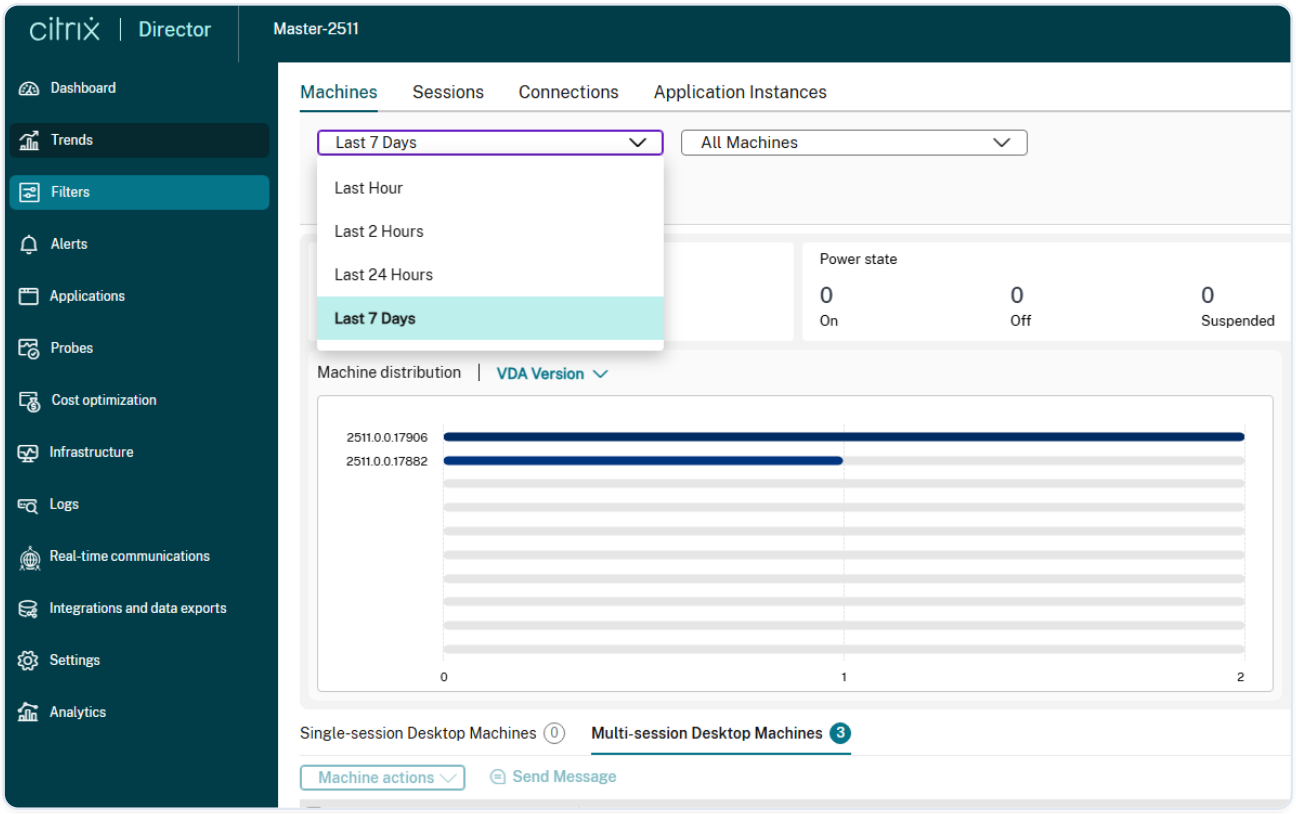
Tabela de Sessão Única/Múltipla: Novas Definições de Coluna



NOME DA COLUNA	DESCRIÇÃO	VALORES POSSÍVEIS
Serviço de Desktop	Estado de integridade do serviço principal responsável pelo gerenciamento da sessão de desktop (por exemplo, CtxSvcHost).	Em Execução, Parado, Não Instalado, Pausado, Inicialização Pendente, Parada Pendente, Continuação Pendente, Pausa Pendente, Desconhecido
Serviço ICA da Citrix	Estado de integridade do serviço principal que lida com o protocolo Independent Computing Architecture (ICA) para sessões de usuário.	Em Execução, Parado, Não Instalado, Pausado, Inicialização Pendente, Parada Pendente, Continuação Pendente, Pausa Pendente, Desconhecido
Mecanismo de Política de Grupo da Citrix	Estado de integridade do serviço responsável pelo processamento e aplicação de políticas específicas da Citrix.	Em execução, Parado, Não instalado, Pausado, Inicialização pendente, Parada pendente, Continuação pendente, Pausa pendente, Desconhecido
Serviço de Gerenciamento de Perfil	Status de saúde do Citrix Profile Management que é usado para gerenciar perfis de usuário em ambientes virtuais Citrix.	Em execução, Parado, Não instalado, Pausado, Inicialização pendente, Parada pendente, Continuação pendente, Pausa pendente, Desconhecido
Saúde da licença MSFT RDS	Indica o status da verificação de licenciamento dos	Em execução, Parado, Não instalado, Pausado,

NOME DA COLUNA	DESCRIÇÃO	VALORES POSSÍVEIS
	Serviços de Área de Trabalho Remota (RDS) da Microsoft.	Inicialização pendente, Parada pendente, Continuação pendente, Pausa pendente, Desconhecido
Serviço de Host do Agente WEM	Status de saúde do agente do Workspace Environment Management (WEM) responsável pela otimização e configuração.	Em execução, Parado, Não instalado, Pausado, Inicialização pendente, Parada pendente, Continuação pendente, Pausa pendente, Desconhecido
Serviços de Área de Trabalho Remota	Status de saúde dos Serviços de Área de Trabalho Remota da Microsoft subjacentes (necessário para a funcionalidade de host de sessão única e multi-sessão).	Em execução, Parado, Não instalado, Pausado, Inicialização pendente, Parada pendente, Continuação pendente, Pausa pendente, Desconhecido
Serviço Uber Agent	Status de saúde do serviço de agente de monitoramento de terceiros (se aplicável e instalado).	Em execução, Parado, Não Instalado, Pausado, Inicialização Pendente, Parada Pendente, Continuação Pendente, Pausa Pendente, Desconhecido

4. Suporte para novos Filtros de Intervalo de Tempo



1. **Últimas 2 Horas**

    - **Objetivo:** Fornece uma visão imediata e de alta granularidade da utilização de recursos do VDA nas últimas 120 minutos.
    - **Utilidade:** Este curto período de tempo é ideal para solução de problemas em tempo real. Use-o para identificar o momento exato em que ocorreu um pico de recursos (como alta CPU ou baixo IOPS de disco) e correlacioná-lo com atividades recentes do usuário ou ações administrativas.

2. Últimos 7 Dias

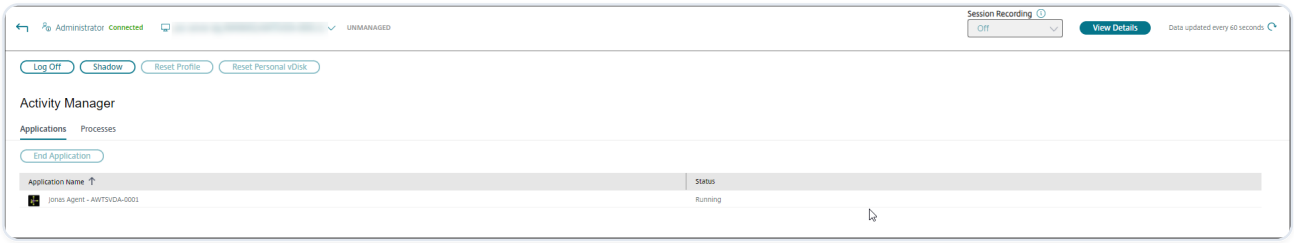
    - **Objetivo:** Exibe o uso de recursos e as tendências de desempenho na última semana.
    - **Utilidade:** Este é o filtro padrão para revisão de desempenho semanal. Ele ajuda os administradores a identificar problemas de desempenho recorrentes, como dias específicos ou horários de pico (por exemplo, logons de segunda-feira de manhã) que consistentemente sobrecarregam os recursos do VDA, permitindo um planejamento de capacidade proativo e otimização.

Métricas de Monitoramento de Integridade do VDA: Plataformas e versões suportadas

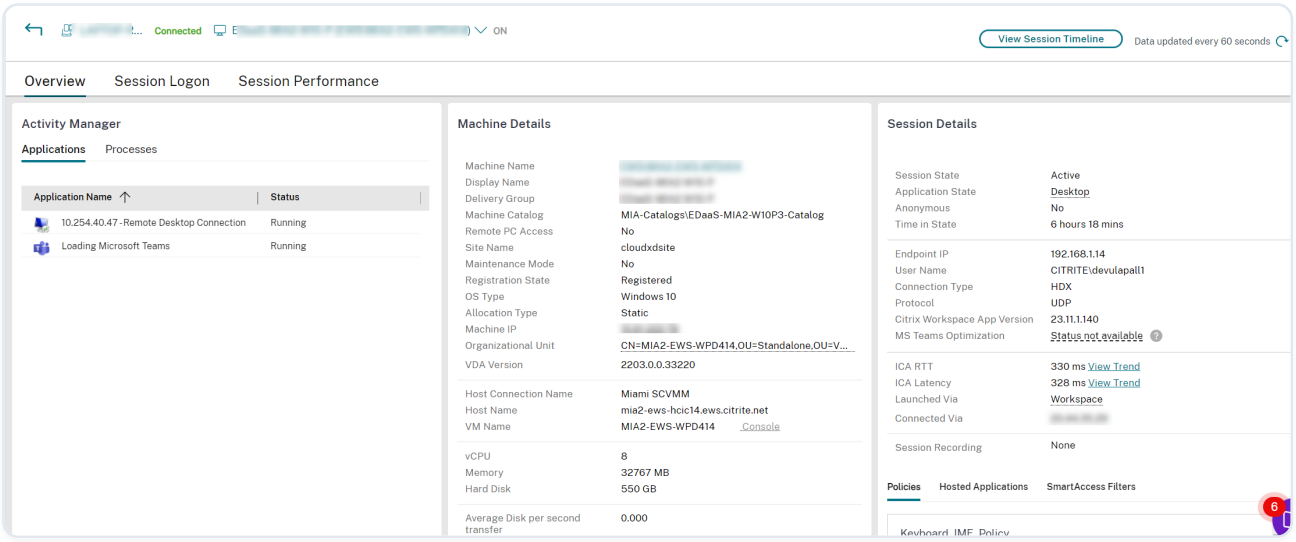
COLUNAS VDA	WINDOWS	MAC	LINUX
Serviço de Área de Trabalho	2511 ou superior	2511 ou superior	2511 ou superior
Serviço ICA do Citrix	2511 ou superior	2511 ou superior	2511 ou superior
Mecanismo de Política de Grupo do Citrix	2511 ou superior	2511 ou superior	2511 ou superior
Serviço de Gerenciamento de Perfil	2511 ou superior	2511 ou superior	2511 ou superior
Saúde da licença MSFT RDS	2511 ou superior	2511 ou superior	2511 ou superior
Serviço de Host do Agente WEM	2511 ou superior	2511 ou superior	2511 ou superior
Serviços de Área de Trabalho Remota	2511 ou superior	2511 ou superior	2511 ou superior
Serviço Uber Agent	2511 ou superior	2511 ou superior	2511 ou superior

Solucionar problemas do usuário

Use a exibição **Help Desk** do Monitor (página **Activity Manager**) para visualizar informações sobre o usuário ou o endpoint.



Clicar em **View Details** no Activity Manager para Usuário abre a página **User Details**. Clicar em **View Details** no Activity Manager para Endpoint abre a página **Endpoint Details**.



Se o usuário tivesse iniciado mais de uma sessão, o seletor de sessão seria exibido.



Escolha uma sessão para visualizar os detalhes.

- Verifique os detalhes sobre a sessão, a experiência de login do usuário, a inicialização da sessão, a conexão e os aplicativos.
- você pode fazer o Shadow da máquina do usuário.
- Solucione o problema com as ações recomendadas na tabela a seguir e, se necessário, encaminhe o problema ao administrador apropriado.

Status de otimização do Microsoft Teams

O Citrix Monitor exibe o status de otimização do Microsoft Teams para sessões HDX™ na página **User Details** > painel **Session Details** > campo **MS Teams Optimization**. O Microsoft Teams

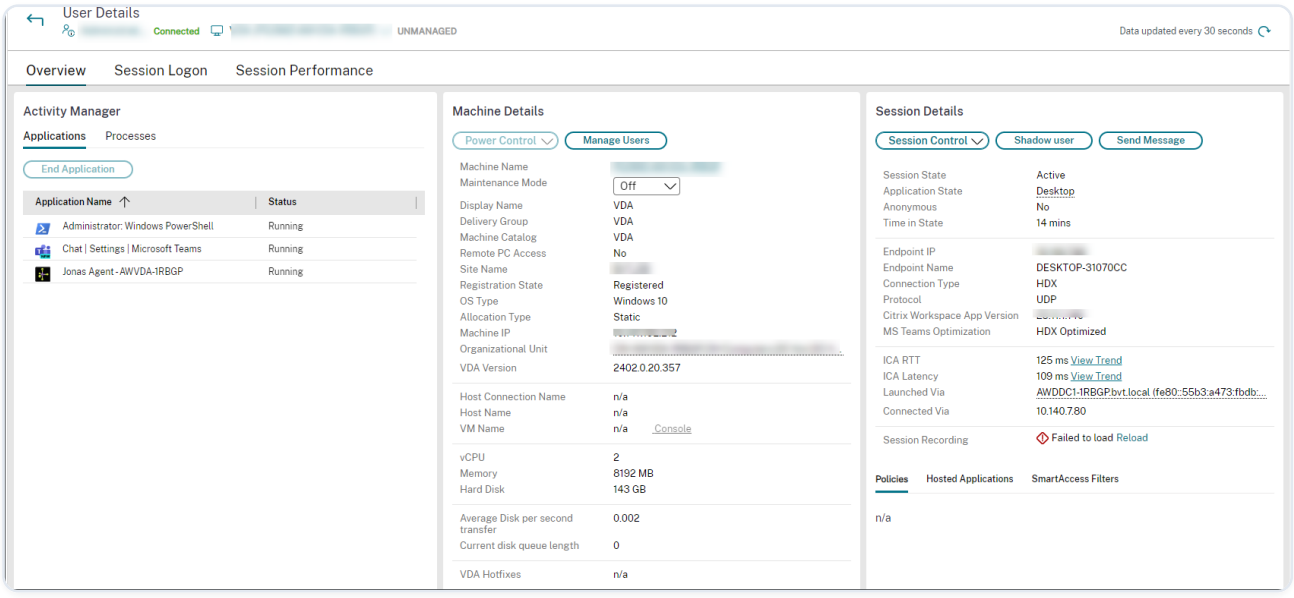
otimizado é fundamental para uma melhor experiência do usuário, como áudio e vídeo nítidos. A visibilidade do status de otimização do Microsoft Teams é útil para reduzir o tempo necessário para resolver tickets e ajuda os administradores a identificar métricas importantes durante a solução de problemas.

Nota:

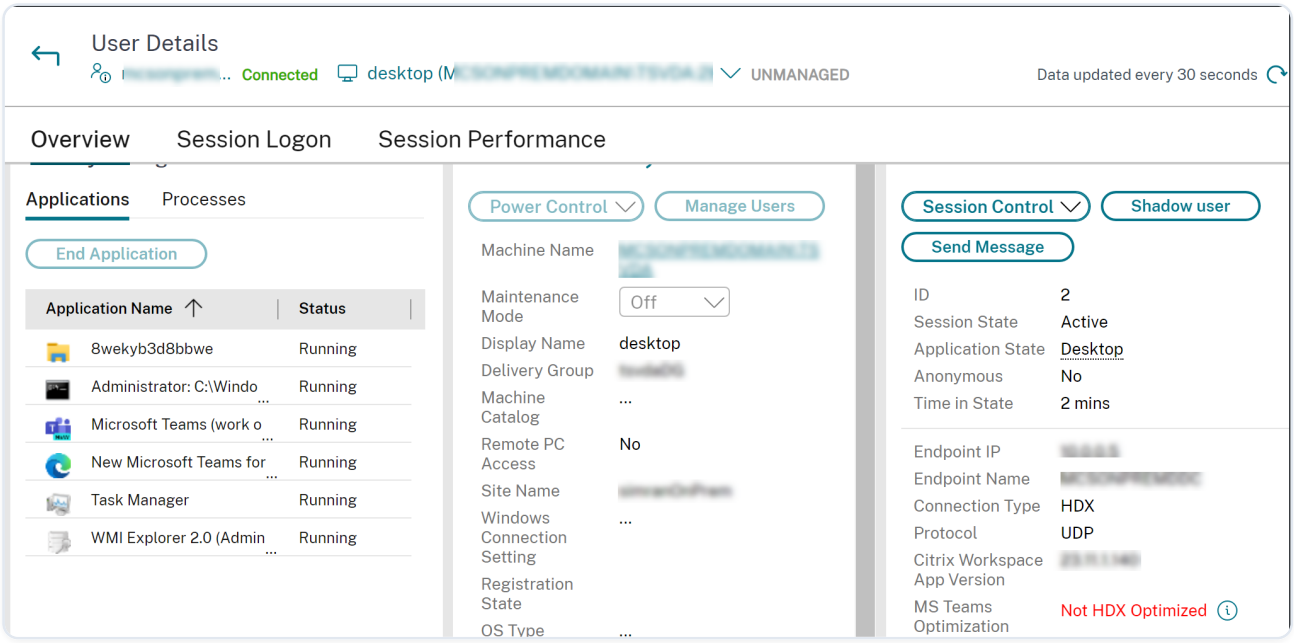
O Citrix Monitor oferece suporte ao Microsoft Teams versão 2.1 ou anterior.

Pré-requisitos:

- Os VDAs estão executando a versão 2311 e posterior.
- As versões compatíveis do aplicativo Citrix Workspace estão listadas em Otimização para Microsoft Teams.
- O Microsoft Teams é executado como um aplicativo publicado ou dentro de um desktop publicado.
- Serviços cruciais, como o Serviço de Redirecionamento de Vídeo HTML5 do Citrix HDX, estão em execução.



Se o Microsoft Teams não estiver otimizado, a dica de ferramenta fornece um link para um artigo de solução de problemas externo ao vivo do HDX contendo dicas para otimizar o Microsoft Teams. Solução de problemas de otimização do HDX.



Dicas de solução de problemas

PROBLEMA DO USUÁRIO	SUGESTÕES
O logon demora muito ou falha intermitentemente ou repetidamente	Diagnosticar problemas de logon do usuário
A inicialização da sessão demora muito ou falha intermitentemente ou repetidamente	Diagnosticar problemas de inicialização da sessão
Identificar os componentes envolvidos no estabelecimento da sessão	Analisar a exibição de Topologia da Sessão
A resposta da sessão está lenta ou não está respondendo	Diagnosticar problemas de desempenho da sessão
O aplicativo está lento ou não está respondendo	Resolver falhas de aplicativo
A conexão falhou	Restaurar conexões de desktop
A sessão está lenta ou não está respondendo	Restaurar sessões
O vídeo está lento ou com baixa qualidade	Executar relatórios do sistema de canal HDX

Nota:

> Para garantir que a máquina não esteja no modo de manutenção, na exibição Detalhes do Usuário, revise o painel Detalhes da Máquina.

Desempenho da Sessão

A guia **Desempenho da Sessão** possui fluxos de trabalho de solução de problemas aprimorados, começando com a capacidade de correlacionar métricas em tempo real na identificação de problemas dentro das sessões do usuário. O painel **Topologia da Sessão** fornece uma representação visual do caminho na sessão para sessões HDX conectadas. O painel **Métricas de Desempenho** fornece tendências para as métricas de sessão como ICARTT, Latência ICA, Quadros por Segundo, Largura de Banda de Saída Disponível e Largura de Banda de Saída Consumida ajudam a indicar como essas métricas se comportaram ao longo do tempo. Para obter mais informações, consulte Diagnosticar problemas de desempenho da sessão.

Dicas de pesquisa

A pesquisa por nome de usuário é realizada em todos os Active Directories configurados.

Quando você digita um nome de máquina multiusuário em um campo de Pesquisa, os Detalhes da Máquina para a máquina especificada são exibidos.

Quando você digita um nome de endpoint em um campo de Pesquisa, as sessões não autenticadas (anônimas) e autenticadas que estão conectadas a um endpoint específico são listadas. Esta lista permite a solução de problemas de sessões não autenticadas. Certifique-se de que os nomes dos endpoints sejam exclusivos para permitir a solução de problemas de sessões não autenticadas.

Os resultados da pesquisa também incluem usuários que não estão usando ou atribuídos a uma máquina atualmente.

- As pesquisas não diferenciam maiúsculas de minúsculas.
- Entradas parciais produzem uma lista de possíveis correspondências.
- Depois de digitar algumas letras de um nome composto, separado por um espaço, os resultados incluem correspondências para ambas as strings. Os exemplos de nomes compostos são nome de usuário, sobrenome e primeiro nome, ou nome de exibição. Por exemplo, se você digitar "jo rob", os resultados podem incluir strings como “John Robertson” ou "Robert Jones".

Para retornar à página inicial, selecione **Gerenciar > Monitorar** no painel esquerdo do Studio.

Diagnosticar falhas de autenticação condicional

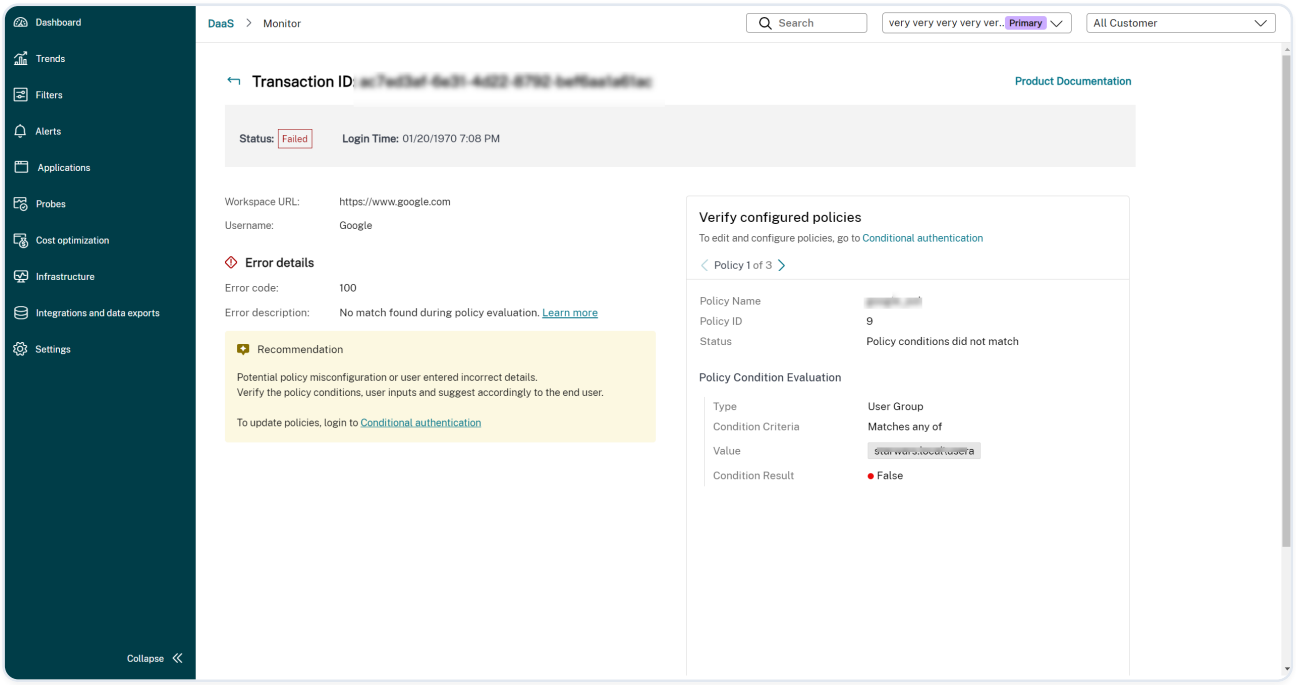
A autenticação condicional permite que os administradores do Citrix Cloud direcionem os usuários finais para diferentes Provedores de Identidade (IdPs) durante o fluxo de login do Workspace com base nas condições de política que você definir. Isso significa que diferentes usuários finais terão níveis variados de verificação de acesso com base nos fatores de risco estabelecidos pelo Administrador. Para obter mais informações sobre autenticação condicional, consulte Autenticação condicional.

Sempre que qualquer autenticação condicional falhar, você pode usar o ID da transação disponível na mensagem de falha e pesquisar no Monitor os detalhes da falha. O Monitor ajuda você a solucionar eventos de falha de autenticação condicional exibindo os motivos da falha e as políticas condicionais na interface do usuário do Monitor.

Visualizando falhas de autenticação condicional

Para visualizar a falha de autenticação condicional, siga estas etapas:

1. Copie o ID da transação para a sessão com falha que usa autenticação condicional.
2. No painel do Monitor, clique em **Pesquisar**.
3. Selecione **ID da Transação** na lista suspensa.
4. Cole o ID da transação copiado. Clique no resultado da pesquisa e a página de detalhes do ID da transação será exibida.



Detalhes do ID da transação

Os seguintes detalhes são exibidos na página de detalhes do ID da transação:

CAMPO	DESCRIÇÃO
Status	Exibe o status da autenticação condicional. Os valores possíveis são *Sucesso* ou *Falha*.
Hora do Login	A hora do login.
URL do Workspace	A URL da loja adicionada ao aplicativo Citrix Workspace™.
Detalhes do Erro	
Código de Erro	Exibe o código de erro. Os possíveis códigos de erro são
	100 - Este erro ocorre quando nenhuma correspondência é encontrada durante a avaliação da política.
	200 - Este é um erro interno. Se o problema persistir, entre em contato com a equipe de suporte da Citrix®.
Descrição do Erro	Exibe a descrição do erro.
Verificar Políticas Configuradas	
Nome da Política	Exibe o nome da política.
ID da Política	Exibe o ID da política.
Status	Exibe o status da política.
Avaliação da Condição da Política	
Tipo	Exibe o tipo de condição da política.
Critérios da Condição	Exibe os critérios da condição.
Valor	Exibe o valor da condição da política.
Resultado da Condição	Exibe o resultado da avaliação da política.

Diagnosticar transações do serviço Device Posture

Os administradores agora podem diagnosticar e solucionar problemas de transações do Serviço Device Posture de forma eficaz. Esta atualização aprimora os recursos de solução de problemas no Citrix Monitor, fornecendo informações detalhadas sobre a avaliação da política do Device Posture, verificações de conformidade e diagnóstico de erros.

Compreendendo o fluxo de avaliação do serviço Device Posture

Um lançamento típico de acesso a aplicativos Secure Private Access ou VDI envolve os três estágios a seguir:

1. **Pré-autenticação**: Uma verificação básica de higiene do endpoint é realizada usando o Serviço Device Posture. O acesso é bloqueado antes da autenticação se um dispositivo não atender às políticas de conformidade.
2. **Autenticação**: Autentica o usuário nesta fase. A autenticação falha se houver incompatibilidade de credenciais ou erros do provedor de identidade.
3. **Acesso ao aplicativo**: Os dois subestágios a seguir estão envolvidos nesta fase:
    - **Estágio de intermediação e enumeração de políticas**: Quando o contexto do dispositivo de um usuário viola as configurações da política, o acesso aos aplicativos é restrito.
    - **Estágio de lançamento do aplicativo**: O estágio final, onde uma transação de aplicativo é concluída usando o Citrix Enterprise Browser™, o cliente Secure Private Access ou o cliente de endpoint nativo.

Aprimoramentos na solução de problemas no Citrix Monitor

Com esta atualização, o Citrix Monitor oferece solução de problemas do Serviço Device Posture baseada em pesquisa, permitindo que as equipes de TI:

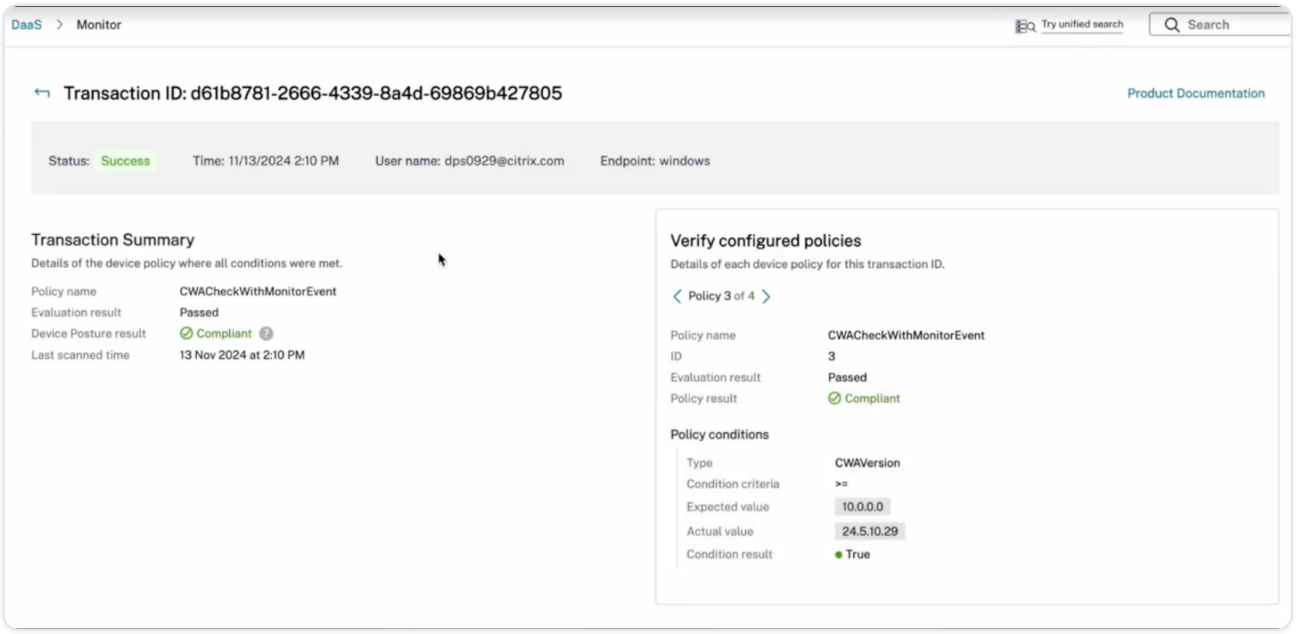
- Filtrar transações por ID de usuário ou ID de transação para depuração direcionada.
- Analisar os resultados da avaliação da política, como se um dispositivo está em conformidade, não em conformidade ou bloqueado devido a violações de política.
- Identificar falhas de política examinando verificações de conformidade detalhadas, valores esperados e valores contextuais em tempo real.
- Revisar metadados do dispositivo, configurações de política e logs para diagnósticos mais aprofundados.
- Identificar transações com falha devido a erros de sistema, com mensagens de erro vinculadas a artigos da base de conhecimento para resolução rápida.

Como as equipes de TI podem usar o aprimoramento da solução de problemas

TRIAGEM DE PROBLEMAS DE POSTURA DO DISPOSITIVO

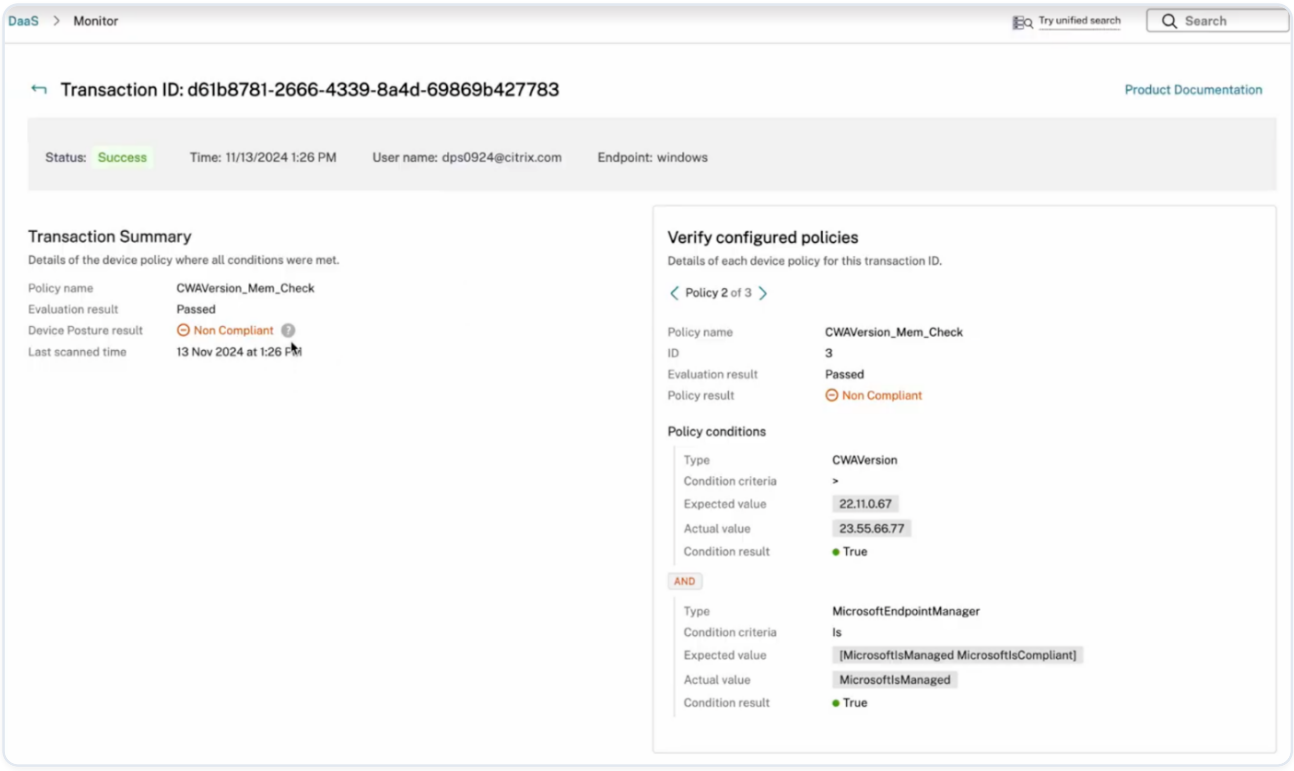
Pesquise um ID de transação relatado pelo usuário para localizar rapidamente os logs relevantes do Serviço de Postura do Dispositivo. Revise se as verificações de conformidade foram aprovadas ou falharam e determine as causas raiz.

Por exemplo, ao pesquisar um ID de transação, você pode revisar o resultado da política de verificação de Postura do Dispositivo — se foi bem-sucedida (compatível ou não compatível) ou falhou devido a um erro. O sistema fornece o contexto completo da avaliação do Serviço de Postura do Dispositivo, incluindo metadados do cliente, detalhes da política e outros detalhes da transação.



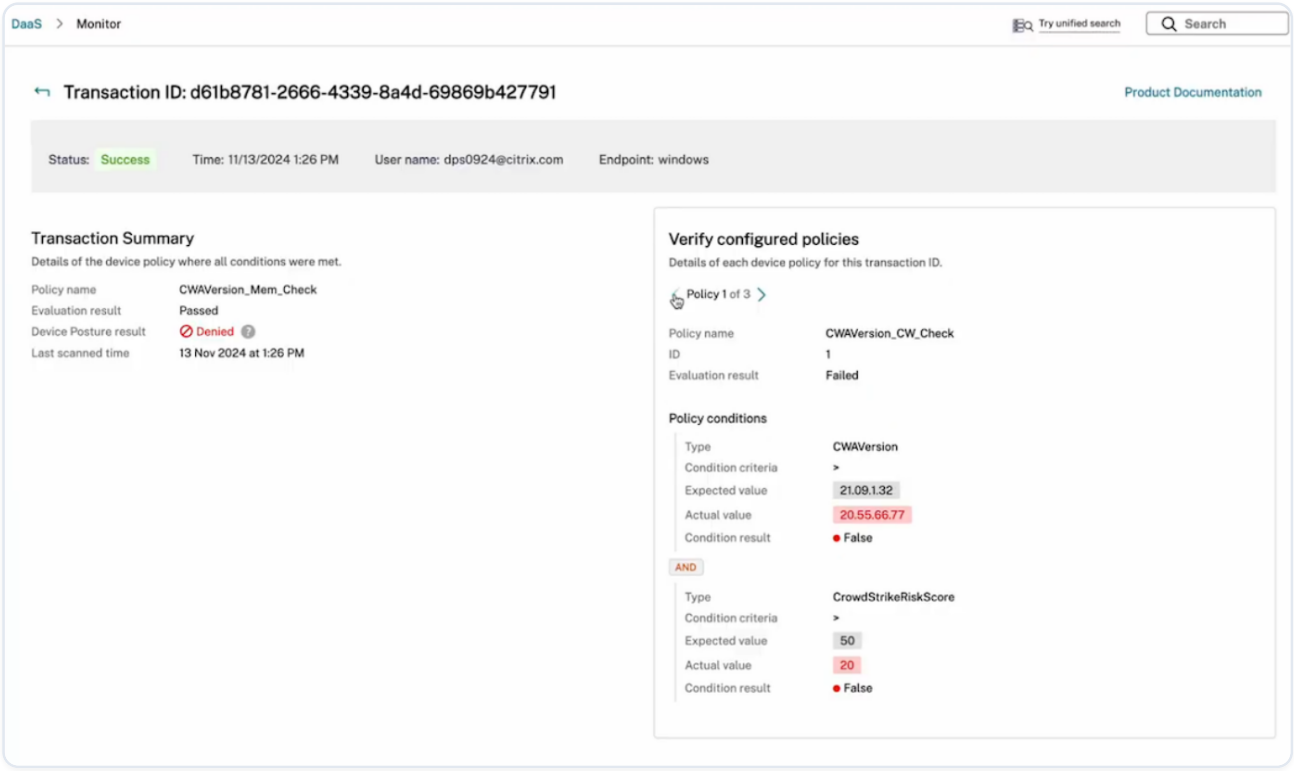
INVESTIGANDO BLOQUEIOS DE ACESSO BASEADOS EM POLÍTICAS

Quando um dispositivo não está em conformidade, a TI pode inspecionar os parâmetros exatos da política que falharam. O sistema fornece comparações lado a lado do valor esperado configurado com os dados em tempo real do dispositivo.

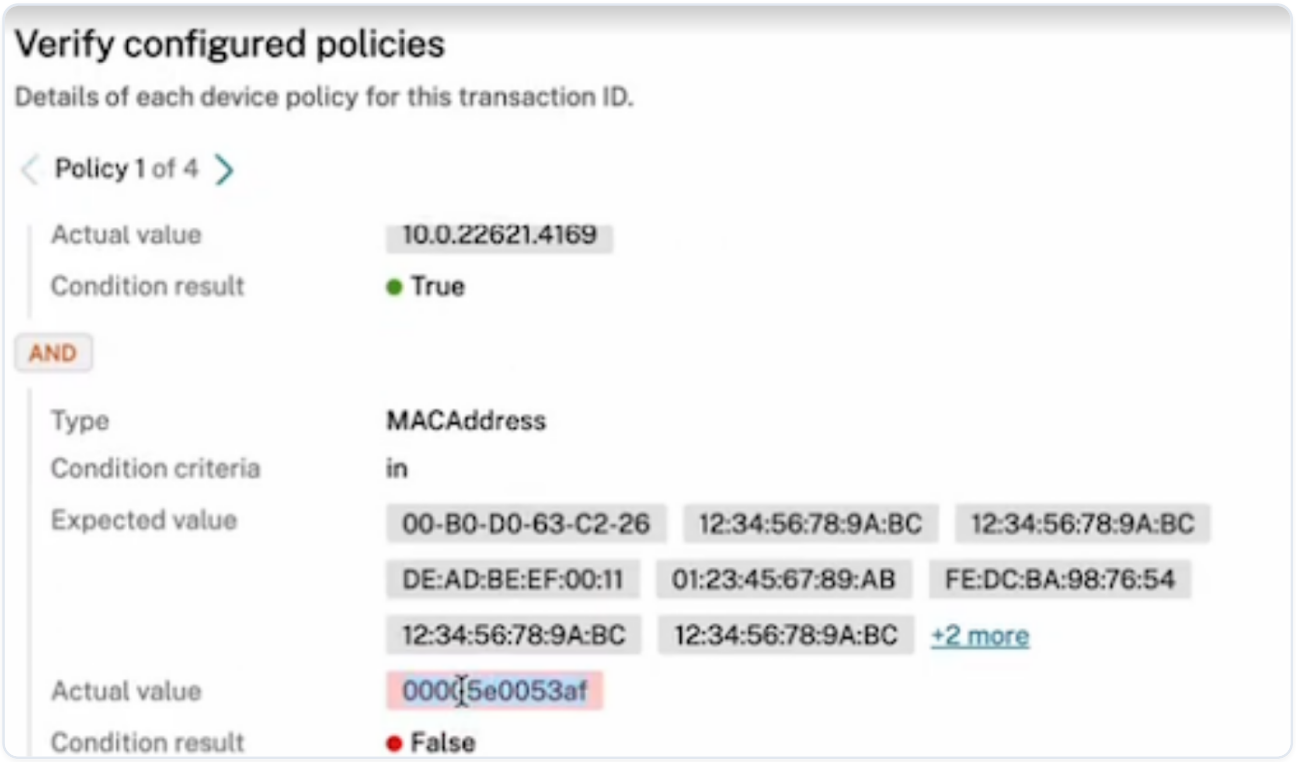


DEPURANDO GRANDES CONJUNTOS DE POLÍTICAS COM PESQUISA DE PRECISÃO

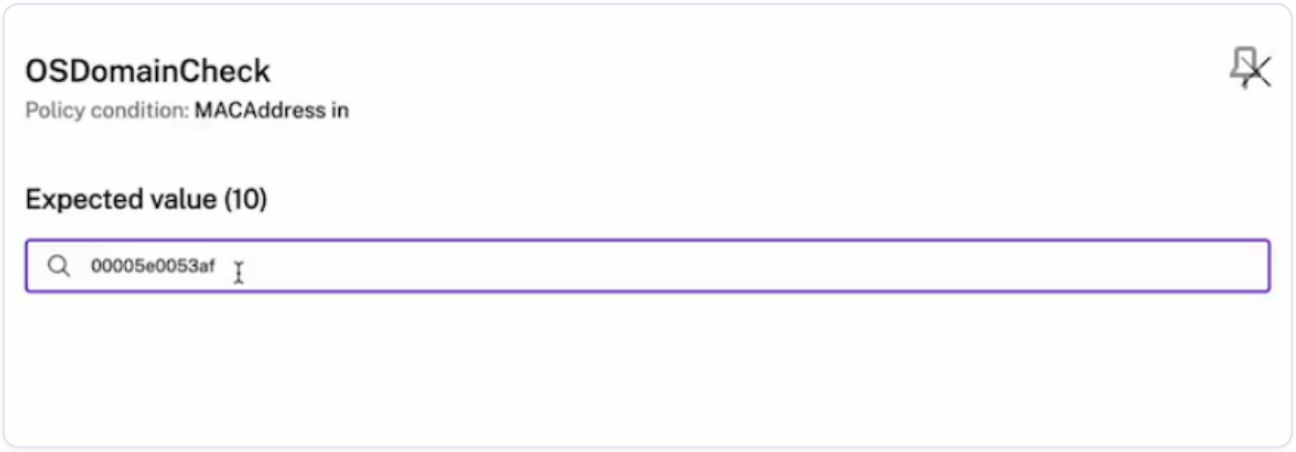
Os administradores podem pesquisar parâmetros específicos em ambientes complexos com várias políticas e verificar se o contexto de usuário esperado está presente. O sistema destaca visualmente a condição de falha se ocorrer uma incompatibilidade de valor de parâmetro, acelerando a identificação da causa raiz. Além disso, os administradores podem navegar pelas políticas para ver quais foram avaliadas e quais geraram o resultado da transação atual.



Para solucionar problemas de grandes conjuntos de parâmetros de política, você pode pesquisar os parâmetros e ver se o contexto de usuário desejado está presente em tempo real.



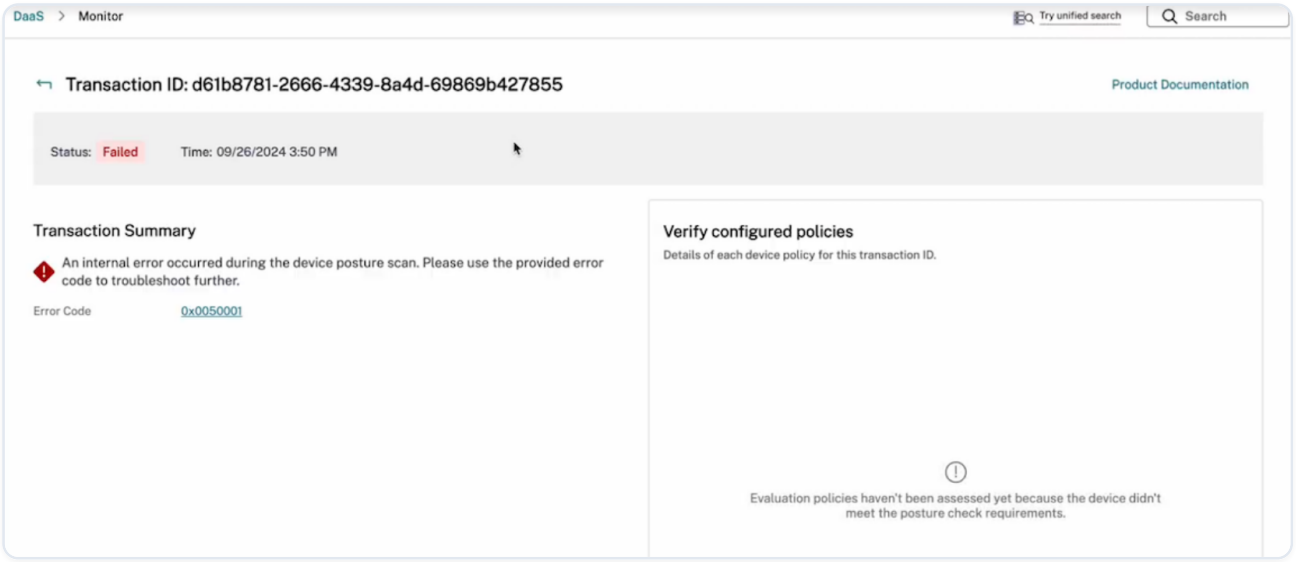
Por exemplo, na captura de tela anterior, o campo destacado, quando pesquisado, não resultou em nenhum resultado (mencionado na imagem a seguir), sugerindo que o valor do parâmetro não correspondia. Essa incompatibilidade fez com que o resultado da condição fosse falso e, falhando nisso, o resultado geral da política fosse negado.



LIDANDO COM FALHAS E ERROS DE TRANSAÇÃO

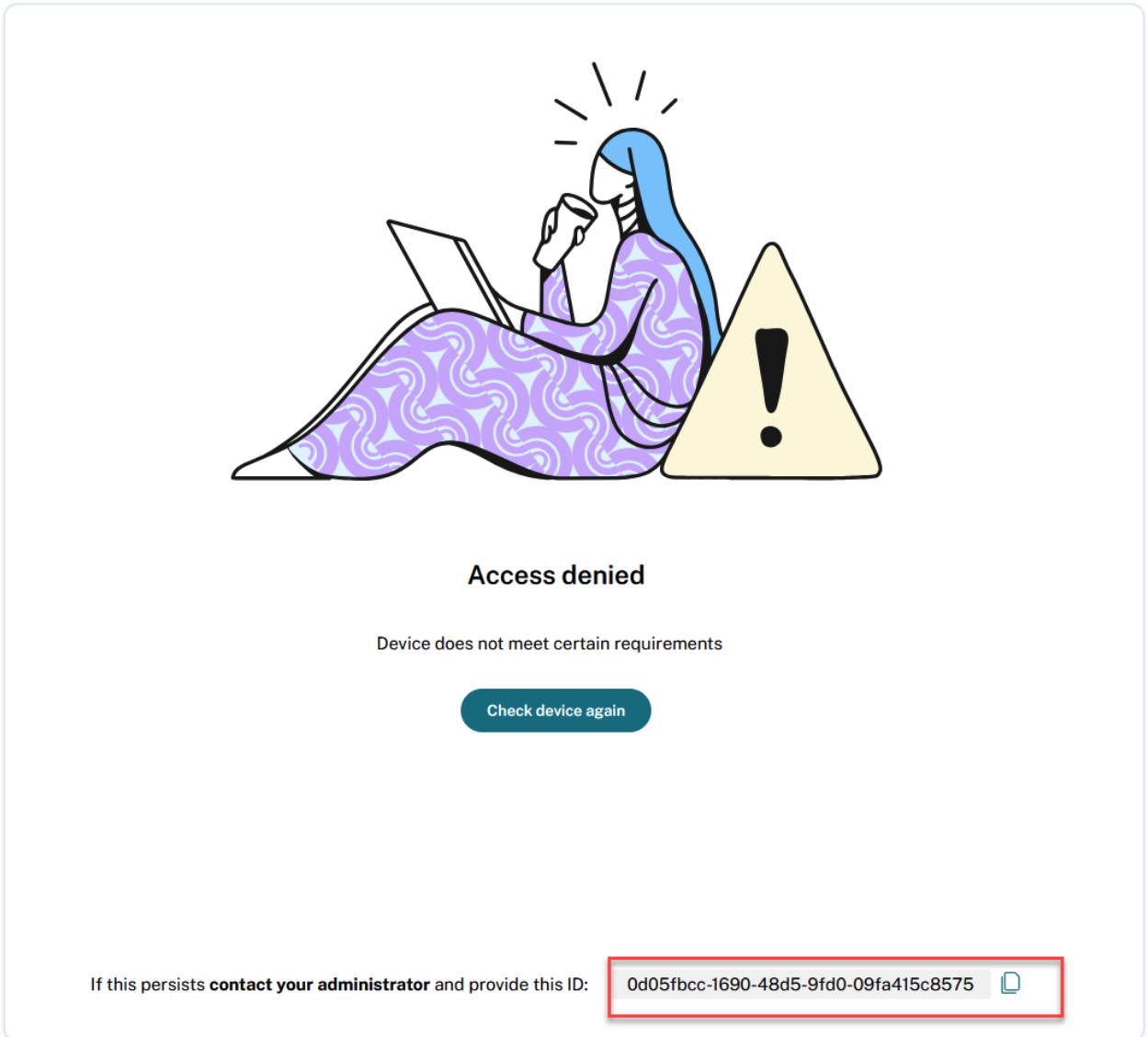
Se uma avaliação de política falhar devido a um erro de sistema, os seguintes detalhes serão exibidos no Citrix Monitor:

- Descrições de erro com detalhes contextuais.
- Links para documentação de solução de problemas, permitindo uma resolução mais rápida.

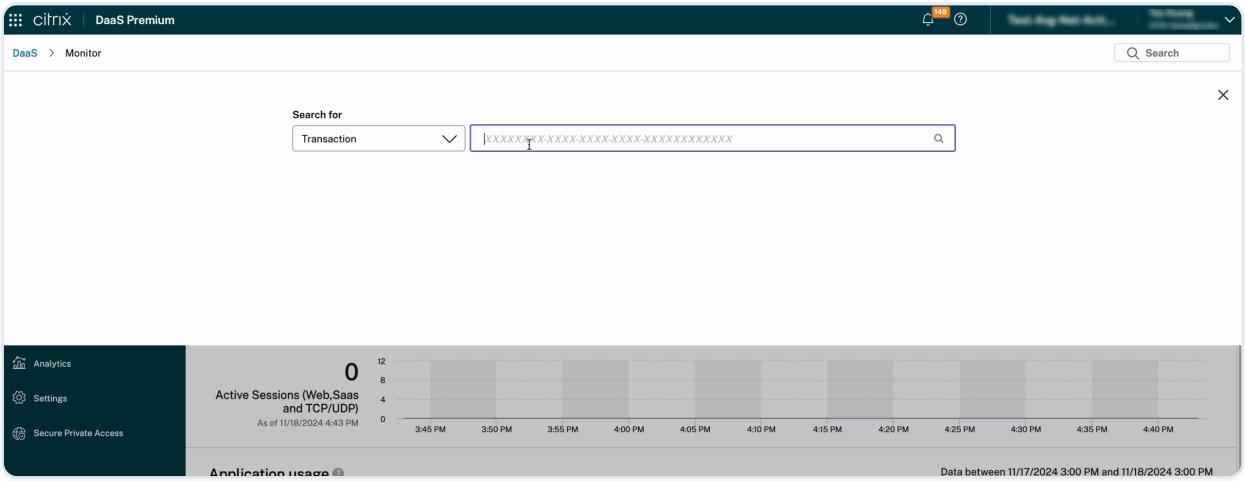


Etapas para diagnosticar transações do Serviço de Postura do Dispositivo

1. Copie o ID da transação da sessão falha ou com acesso negado do dispositivo do usuário final.



2. Faça login no Citrix Cloud.
3. No bloco DaaS, clique em **Gerenciar** e, em seguida, clique na guia **Monitor**.
4. Insira o ID da transação no campo **Pesquisar** e clique em **Detalhes**.



Você pode visualizar o resumo da transação e os detalhes de verificação das políticas de Postura do Dispositivo configuradas. Os diferentes valores para avaliação de política são compatível, não compatível e negar.

RESUMO DA TRANSAÇÃO

A página **Resumo da Transação** fornece o resultado da política de Postura do Dispositivo. Para resultados compatíveis, não compatíveis e negados, o resumo inclui:

- **Plataforma**: O SO do dispositivo cliente.
- **Nome da política**: Nome da política de Postura do Dispositivo.
- **Resultado da avaliação**: Indica se a política de Postura do Dispositivo foi aprovada ou falhou.
- **Resultado da Postura do Dispositivo**: Indica se o resultado da Postura do Dispositivo é compatível, não compatível ou negado.
- **Última verificação**: A hora em que o dispositivo foi verificado pela última vez.

VERIFICAR POLÍTICAS CONFIGURADAS

A seção **Verificar Políticas Configuradas** fornece detalhes abrangentes da avaliação da política, incluindo:

- Razões para a falha.
- A regra específica que falhou.
- Evidências coletadas.

Essas informações permitem que os administradores solucionem problemas e tomem as ações apropriadas com base nos detalhes da política.

Processo de avaliação da política de postura do dispositivo

1. **Falha da política e identificação da regra**:
   - Identifique qual regra falhou e por que falhou.
   - Coletar evidências relacionadas à falha.
2. **Determinação do resultado**:
   - Dependendo da avaliação da política, o resultado pode ser compatível, não compatível ou negado.
   - Se nenhuma política corresponder, o resultado é "nenhuma política correspondente".
3. **Visualizando detalhes da política**:
   - Os administradores podem visualizar os detalhes de cada política de dispositivo para um ID de transação específico.
   - Use as setas para trás e para frente para navegar entre as diferentes políticas.

   Em casos de resultados compatíveis, não compatíveis e negados, a avaliação da política de Postura do Dispositivo inclui as seguintes informações na seção Verificar Políticas Configuradas:

   - **Nome da política**: Nome da política do dispositivo.
   - **ID**: A ordem em que a política é avaliada.
   - **Resultado da avaliação**: Indica se a política de Postura do Dispositivo foi aprovada ou falhou.
   - **Resultado da política**: Indica se o resultado da Postura do Dispositivo é compatível, não compatível ou negado.
   - **Condições da política**:
     - **Tipo**: O tipo de verificação do dispositivo.
     - **Critérios de condição**: A condição para avaliar a regra da política.
     - **Valor esperado**: O valor configurado da condição da política.
     - **Valor real**: A evidência coletada do endpoint.
     - **Resultado da condição**: Indica se a condição foi aprovada ou falhou.

Código de erro

Quando há um problema e o Device Posture não consegue avaliar a política, o código de erro é exibido.

Se houver uma falha, copie o código de erro e entre em contato com o suporte da Citrix.

Os detalhes da política e os códigos de erro simplificam a triagem e a solução de problemas do usuário.

A tabela a seguir fornece o código de erro, a mensagem de erro e a solução para o erro:

# Nº	MENSAGEM DE ERRO	CÓDIGO DE ERRO	AÇÃO
1	Falha ao ler as políticas configuradas.	0x0050001	Entre em contato com o Suporte Citrix
2	Falha ao avaliar verificações de endpoint.	0x0050002	Entre em contato com o Suporte Citrix
3	Falha ao processar políticas ou expressão.	0x0050003	Entre em contato com o Suporte Citrix
4	Falha ao salvar detalhes do endpoint.	0x0050004	Entre em contato com o Suporte Citrix
5	Falha ao processar resultados de verificação de endpoints.	0x0050005	Entre em contato com o Suporte Citrix
6	Falha ao ler a configuração do modo de Postura do Dispositivo.	0x0050006	Entre em contato com o Suporte Citrix

Diagnosticar problemas de inicialização de sessão

Além das fases do processo de logon mencionadas na seção Diagnosticar problemas de logon do usuário, o Monitor exibe a duração da inicialização da sessão. Essa duração é dividida em duração de inicialização da sessão do Workspace App e duração de inicialização da sessão VDA nas páginas **Detalhes do Usuário** e **Detalhes do Ponto de Extremidade**. Essas duas durações contêm ainda fases individuais cujas durações de inicialização também são exibidas. Esses dados ajudam você a entender e solucionar problemas de alta duração de inicialização da sessão. Além disso, a duração de cada fase envolvida na inicialização da sessão ajuda na solução de problemas associados a fases individuais. Por exemplo, se o tempo de Mapeamento de Unidade for alto, você pode verificar se todas as unidades válidas estão mapeadas corretamente no GPO ou script.

Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos para que os dados de duração da inicialização da sessão sejam exibidos:

- VDA 1903 ou posterior.
- O serviço Citrix End User Experience Monitoring (EUEM) deve estar em execução no VDA.

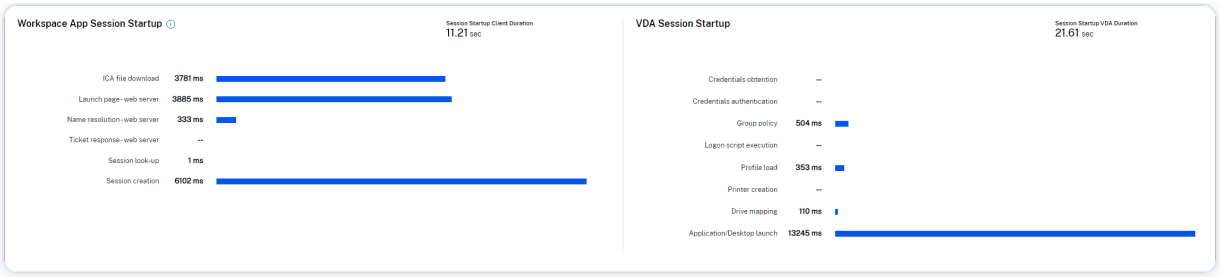
Limitações

As seguintes limitações se aplicam quando o Monitor exibe os dados de duração da inicialização da sessão:

- A duração da inicialização da sessão está disponível apenas para sessões HDX™.
- Para inicializações de sessão de iOS e Android OS, apenas a Duração de Inicialização do VDA está disponível.
- O IFDCD está disponível apenas quando o Workspace App é detectado ao iniciar a partir de um navegador.
- Para inicializações de sessão de macOS, o IFDCD está disponível apenas para o Workspace App 1902 e posterior.
- Para inicializações de sessão de Windows OS, o IFDCD está disponível para o Workspace app 1902 e posterior. Para versões anteriores, o IFDCD é exibido apenas para inicializações de aplicativos a partir de um navegador com o Workspace app detectado.

> **Observações:**

- Se você enfrentar problemas na exibição da duração da inicialização das sessões depois que os pré-requisitos forem atendidos, visualize os logs do servidor Monitor e VDA conforme descrito em CTX130320. Para sessões compartilhadas (vários aplicativos iniciados na mesma sessão), as métricas de Inicialização do Workspace App são exibidas para a conexão mais recente ou o lançamento de aplicativo mais recente.
- Algumas métricas na Inicialização da Sessão VDA não são aplicáveis em reconexões. Nesses casos, uma mensagem é exibida.



Fases de inicialização da sessão do Workspace App

DURAÇÃO DO CLIENTE DE INICIALIZAÇÃO DA SESSÃO (SSCD)

Quando essa métrica é alta, indica um problema do lado do cliente que está causando tempos de inicialização longos. Revise as métricas subsequentes para determinar a provável causa raiz do problema. O SSCD começa o mais próximo possível do momento da solicitação (clique do mouse) e termina quando a conexão ICA® entre o dispositivo cliente e o VDA é estabelecida. Para uma sessão compartilhada, essa duração é muito menor, pois grande parte dos custos de configuração associados à criação de uma nova conexão com o servidor não são incorridos. No próximo nível, há várias métricas detalhadas disponíveis.

DURAÇÃO DO DOWNLOAD DO ARQUIVO ICA (IFDCD)

O IFDCD é o tempo que o cliente leva para baixar o arquivo ICA do servidor. O processo geral é o seguinte:

1. O usuário clica em um recurso (aplicativo ou desktop) no Workspace Application.
2. Uma solicitação do usuário é enviada ao StoreFront através do Citrix Gateway (se configurado), que envia a solicitação ao Delivery Controller.
3. O Delivery Controller encontra uma máquina disponível para a solicitação e envia as informações da máquina e outros detalhes para o StoreFront. Além disso, o StoreFront solicita e recebe um tíquete único da Secure Ticket Authority.
4. O StoreFront gera um arquivo ICA e o envia ao usuário via Citrix Gateway (se configurado).

O IFDCD representa o tempo que leva para o processo completo (etapas 1–4). A duração do IFDCD para de contar quando o cliente recebe o arquivo ICA.

LPWD é o componente StoreFront do processo.

Se o IFDCD for alto (mas o LPWD for normal), o processamento do lançamento no lado do servidor foi bem-sucedido, mas houve problemas de comunicação entre o dispositivo cliente e o StoreFront. Isso resulta de problemas de rede entre as duas máquinas. Portanto, você pode solucionar problemas de rede potenciais primeiro.

DURAÇÃO DO SERVIDOR WEB DA PÁGINA DE LANÇAMENTO (LPWD)

Este é o tempo levado para processar a página de lançamento (launch.aspx) no StoreFront. Se o LPWD for alto, pode haver um gargalo no StoreFront.

As possíveis causas incluem:

- Alta carga no StoreFront. Tente identificar a causa da lentidão verificando os logs do Internet Information Services (IIS) e ferramentas de monitoramento, Gerenciador de Tarefas, Monitor de Desempenho e assim por diante.
- O StoreFront está com problemas para se comunicar com outros componentes, como o Delivery Controller. Verifique se a conexão de rede entre o StoreFront e o Delivery Controller está lenta ou se alguns Delivery Controllers estão inativos ou sobrecarregados.

DURAÇÃO DO SERVIDOR WEB DE RESOLUÇÃO DE NOMES (NRWD)

Este é o tempo levado pelo Delivery Controller para resolver o nome de um aplicativo/desktop publicado para um endereço IP de Máquina VDA.

Quando esta métrica é alta, indica que o Delivery Controller está demorando muito para resolver o nome de um aplicativo publicado para um endereço IP. As possíveis causas incluem:

- um problema no cliente
- problemas com o Delivery Controller, como o Delivery Controller estar sobrecarregado, ou um problema com o link de rede entre eles

DURAÇÃO DO SERVIDOR WEB DE RESPOSTA DE TICKET (TRWD)

Esta duração indica o tempo que leva para obter um ticket (se necessário) do Servidor Secure Ticket Authority (STA) ou do Delivery Controller. Quando esta duração é alta, indica que o servidor STA ou o Delivery Controller estão sobrecarregados.

DURAÇÃO DA PESQUISA DE SESSÃO DO CLIENTE (SLCD)

Esta duração representa o tempo levado para consultar cada sessão para hospedar o aplicativo publicado solicitado. A verificação é realizada no cliente para determinar se uma sessão existente pode manipular a solicitação de inicialização do aplicativo. O método usado depende se a sessão é nova ou compartilhada.

DURAÇÃO DA CRIAÇÃO DE SESSÃO DO CLIENTE (SCCD)

Esta duração representa o tempo levado para criar uma sessão, desde o momento em que o wfica32.exe (ou um arquivo equivalente similar) é iniciado até o momento em que a conexão é estabelecida.

Fases de inicialização da sessão VDA

DURAÇÃO DA INICIALIZAÇÃO DA SESSÃO VDA (SSVD)

Esta duração é a métrica de alto nível de inicialização da conexão do lado do servidor que indica o tempo que o VDA leva para realizar toda a operação de inicialização. Quando esta métrica é alta, indica que há um problema no VDA que aumenta os tempos de inicialização da sessão. Isso inclui o tempo gasto no VDA realizando toda a operação de inicialização.

DURAÇÃO DA OBTENÇÃO DE CREDENCIAIS VDA (COVD)

O tempo que o VDA leva para obter as credenciais do usuário.

Esta duração pode ser artificialmente inflacionada se um usuário não fornecer as credenciais em tempo hábil e, portanto, não for incluída na Duração de Inicialização do VDA. Este tempo provavelmente será significativo apenas se o login manual estiver sendo usado e a caixa de diálogo de credenciais do lado do servidor for exibida (ou se um aviso legal for exibido antes do início do login).

DURAÇÃO DA AUTENTICAÇÃO DE CREDENCIAIS VDA (CAVD)

Este é o tempo que o VDA leva para autenticar as credenciais do usuário contra o provedor de autenticação, que pode ser Kerberos, Active Directory ou uma Interface de Provedor de Suporte de Segurança (SSPI).

DURAÇÃO DA POLÍTICA DE GRUPO VDA (GPVD)

Esta duração é o tempo levado para aplicar objetos de política de grupo durante o logon.

DURAÇÃO DA EXECUÇÃO DE SCRIPT DE LOGIN VDA (LSVD)

Este é o tempo que o VDA leva para executar os scripts de login do usuário.

Você pode tornar os scripts de login do usuário ou grupo assíncronos. Otimize quaisquer scripts de compatibilidade de aplicativos ou use variáveis de ambiente em vez disso.

DURAÇÃO DO CARREGAMENTO DE PERFIL VDA (PLVD)

Este é o tempo que o VDA leva para carregar o perfil do usuário.

Se essa duração for alta, revise sua configuração de Perfil de Usuário. O tamanho e a localização do perfil móvel contribuem para inícios de sessão lentos. Quando um usuário faz logon em uma sessão onde perfis móveis de Serviços de Terminal e pastas pessoais estão habilitados, o conteúdo do perfil móvel e o acesso a essa pasta são mapeados durante o logon, o que consome recursos extras. Às vezes, isso pode consumir uma quantidade significativa do uso da CPU. Use as pastas **Terminal Services home** com pastas pessoais redirecionadas para mitigar esse problema. Em geral, use o Citrix Profile Management para gerenciar perfis de usuário em ambientes Citrix. Se você estiver usando o Citrix Profile Management e tiver tempos de logon lentos, verifique se o seu software antivírus está bloqueando a ferramenta Citrix Profile Management.

DURAÇÃO DA CRIAÇÃO DE IMPRESSORA VDA (PCVD)

Este é o tempo que o VDA leva para mapear as impressoras cliente do usuário de forma síncrona. Se a configuração estiver definida para que a criação da impressora seja realizada de forma assíncrona, nenhum valor é registrado para PCVD, pois isso não afeta a conclusão do início da sessão.

O tempo excessivo gasto no mapeamento de impressoras é frequentemente o resultado das configurações da política de criação automática de impressoras. O número de impressoras adicionadas localmente nos dispositivos cliente dos usuários e sua configuração de impressão podem afetar diretamente os tempos de início da sessão. Quando uma sessão é iniciada, o Citrix Virtual Apps and Desktops™ precisa criar cada impressora mapeada localmente no dispositivo cliente. Reconfigure suas políticas de impressão para reduzir o número de impressoras que são criadas, especificamente quando os usuários têm muitas impressoras locais. Para fazer isso, edite a política de criação automática de impressoras no Delivery Controller e no Citrix Virtual Apps and Desktops.

DURAÇÃO DO MAPEAMENTO DE UNIDADE VDA (DMVD)

Este é o tempo que o VDA leva para mapear as unidades, dispositivos e portas cliente do usuário.

Certifique-se de que suas políticas base incluam configurações para desabilitar canais virtuais não utilizados, como mapeamento de áudio ou porta COM, para otimizar o protocolo ICA e melhorar o desempenho geral da sessão.

DURAÇÃO DO LANÇAMENTO DE APLICATIVO/DESKTOP VDA (ALVD/DLVD)

Esta fase é uma combinação da duração de userinit e Shell. Quando um usuário faz logon em uma máquina Windows, o Winlogon executa userinit.exe. O Usernit.exe executa scripts de logon,

restabelece conexões de rede e, em seguida, inicia explorer.exe, a interface de usuário do Windows. userinit representa a duração entre o início de userinit.exe e o início da interface de usuário para o desktop virtual ou aplicativo. A duração do Shell é o tempo entre a inicialização da interface de usuário e o momento em que o usuário recebe o controle do teclado e do mouse.

DURAÇÃO DA CRIAÇÃO DE SESSÃO VDA (SCVD)

Este tempo inclui atrasos diversos na criação da sessão no VDA.

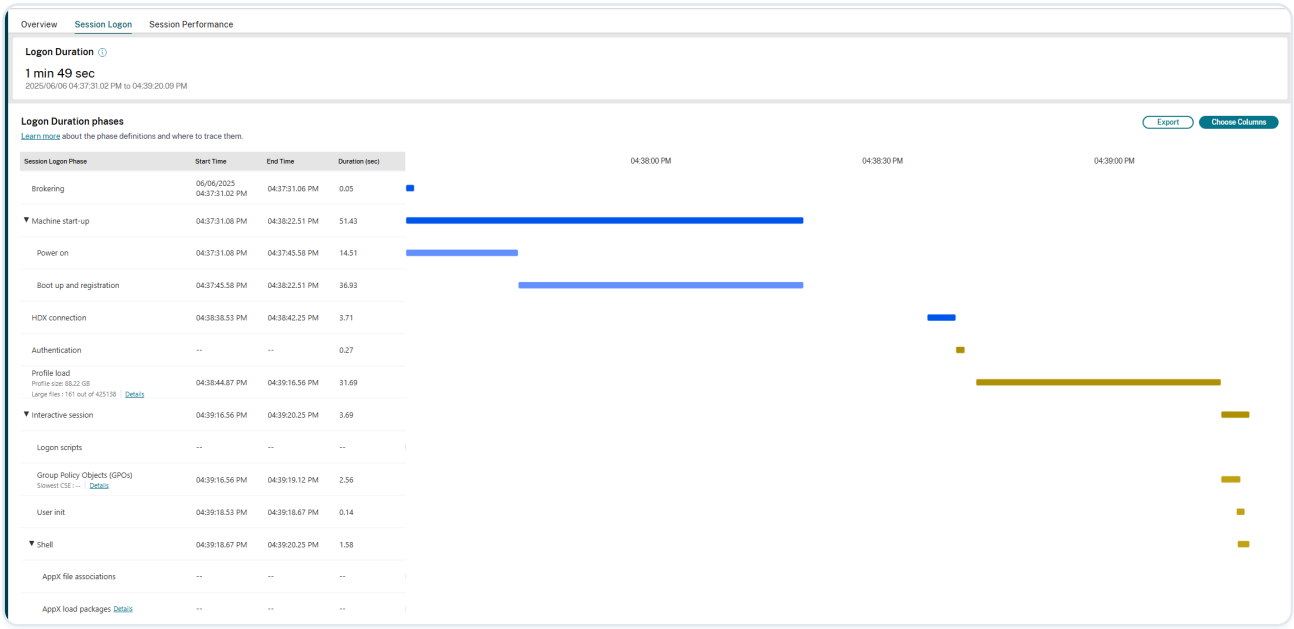
Diagnosticar problemas de logon do usuário

A exibição **Detalhes do Usuário** > guia **Logon da Sessão** exibe uma visão abrangente do processo de logon da sessão. Você pode usar os dados de Duração do Logon para solucionar problemas de logon do usuário.

A duração do logon é medida apenas para conexões iniciais a um desktop ou aplicativo usando HDX. Esses dados não incluem usuários tentando se conectar com o Protocolo de Área de Trabalho Remota ou reconectar-se de sessões desconectadas. Especificamente, a duração do logon não é medida quando um usuário se conecta inicialmente usando um protocolo não-HDX e se reconecta usando HDX.

À medida que os usuários fazem logon no Citrix DaaS™, o Serviço de Monitoramento rastreia as fases do processo de logon. As fases começam a partir do momento em que o usuário se conecta do aplicativo Citrix Workspace™ até o momento em que o desktop está pronto para uso.

A guia **Logon da Sessão** contém o gráfico de fases de Duração do Logon com as várias fases de logon plotadas. A Duração do Logon representa o tempo gasto para estabelecer a conexão e obter um aplicativo ou um desktop do Cloud Connector e o tempo gasto para autenticar e fazer logon em um aplicativo ou desktop virtual. As informações de duração são apresentadas em segundos (ou frações de segundos).



O gráfico de fases de Duração do Logon fornece uma visão clara das diferentes fases de logon e seus tempos de início e término. O gráfico mostra a sobreposição das fases de logon individuais. O tempo total de logon pode não ser a soma das durações das fases de logon individuais. Isso ocorre porque as fases individuais podem se sobrepor e nem todas as fases de logon fazem parte desta representação. Além disso, certas fases podem se estender mesmo depois que o usuário começa a interagir com o aplicativo ou desktop virtual, e essa duração não é medida como parte da duração geral do logon.

Use esta exibição para identificar fases de logon específicas que causam um atraso no lançamento da sessão. A definição para cada fase de logon e a fonte do evento de onde você pode rastrear informações ajuda na solução de problemas. Ao passar o mouse sobre o gráfico, uma dica de ferramenta é exibida, contendo a duração da fase para a sessão atual, bem como a média de 7 dias do usuário e a média de 7 dias do grupo de entrega. Essas informações ajudam a comparar a duração do logon da sessão atual com os valores médios de 7 dias. Você pode detalhar ainda mais as medições de subfase no caso de GPO e Detalhes do Perfil. Essa visualização ajuda a entender e solucionar facilmente problemas relacionados à duração do logon.

Pré-requisitos

Certifique-se de que os seguintes pré-requisitos sejam atendidos para que os dados de duração do logon e os detalhamentos apareçam:

1. Instale o **Citrix User Profile Manager** e o **Citrix User Profile Manager WMI Plugin** no VDA.
2. Certifique-se de que o Serviço de Gerenciamento de Perfil do Citrix esteja em execução.
3. Para sites XenApp e XenDesktop 7.15 e anteriores, desative a configuração de GPO, **Não processar a lista de execução herdada**.

4. O rastreamento de processo de auditoria deve ser habilitado para o detalhamento da Sessão Interativa.
5. Para o detalhamento de GPO, aumente o tamanho dos logs operacionais da Política de Grupo.

> **Nota:**
>
> A duração do logon é suportada apenas no shell padrão do Windows (explorer.exe) e não em shells personalizados.

Etapas para solucionar problemas de logon do usuário

1. Na exibição **Detalhes do Usuário**, solucione o estado do logon usando o painel Duração do Logon.
    - Se o usuário estiver fazendo logon, a exibição reflete o processo de logon.
    - Se o usuário estiver logado, o painel Duração do Logon exibe o tempo que o usuário levou para fazer logon na sessão atual.
2. Examine as fases do processo de logon.

Fases do processo de logon

INTERMEDIAÇÃO

Tempo levado para decidir qual desktop atribuir ao usuário.

INICIALIZAÇÃO DA MÁQUINA

Se a sessão exigiu o início de uma máquina, este é o tempo levado para iniciar a máquina virtual. A subseção a seguir fornece um detalhamento do tempo levado para iniciar uma máquina virtual durante diferentes fases:

- Ligar - Exibe o tempo levado para ligar uma máquina virtual
- Inicialização e registro - Exibe o tempo levado para inicializar e registrar uma máquina virtual

Você pode usar o botão recolhível para recolher ou expandir as opções em **Inicialização da Máquina**.

CONEXÃO HDX

Tempo necessário para concluir as etapas exigidas na configuração da conexão HDX do cliente para a máquina virtual.

AUTENTICAÇÃO

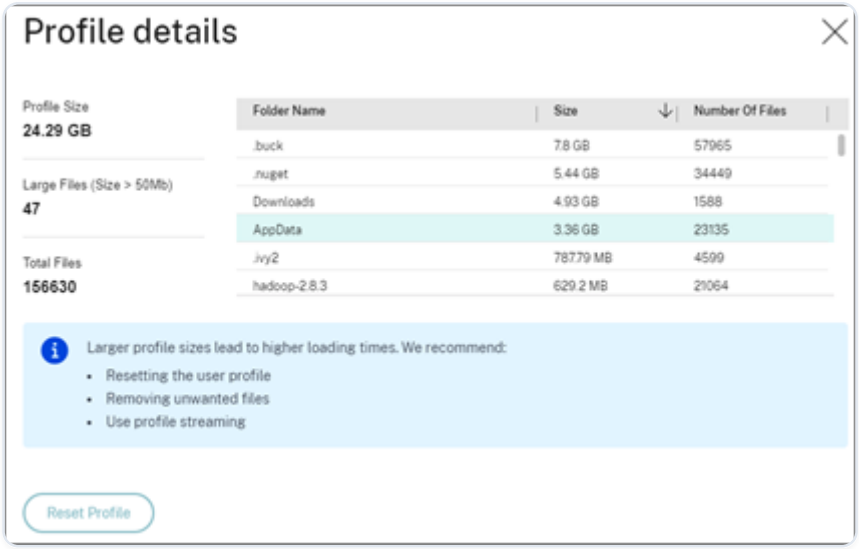
Tempo necessário para concluir a autenticação na sessão remota.

CARREGAMENTO DE PERFIL

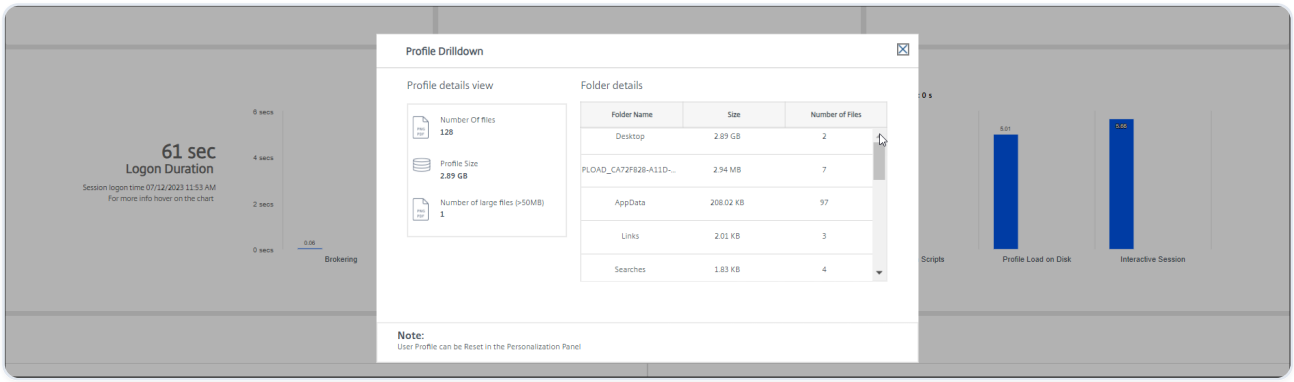
Se as configurações de perfil estiverem configuradas para o usuário ou a máquina virtual, este é o tempo necessário para o perfil carregar.

Se o Citrix Profile Management e o FSLogix estiverem configurados, a barra de Carregamento de Perfil incluirá o tempo gasto pelo Citrix Profile Management e pelo FSLogix para processar perfis de usuário. Esta informação ajuda os administradores a solucionar problemas de alta duração de processamento de perfil. Quando o Profile Management e o FSLogix estão configurados, a barra de Carregamento de Perfil exibe uma duração aumentada. Este aumento é causado por esta melhoria e não reflete uma degradação de desempenho. Esta melhoria está disponível nas versões VDA 2407 ou posteriores.

Ao passar o mouse sobre a barra de Carregamento de Perfil, é exibida uma dica de ferramenta mostrando os detalhes do perfil do usuário para a sessão atual. Esta informação adicional pode ajudar a solucionar problemas de alto carregamento de perfil.



Clique em **Detalhes** para aprofundar ainda mais em cada pasta individual na pasta raiz do perfil (por exemplo, C:/Users/username), seu tamanho e o número de arquivos (incluindo arquivos dentro de pastas aninhadas).



O detalhamento do perfil está disponível em VDAs 1811 e posteriores. Usando as informações de detalhamento do perfil, você pode resolver problemas que envolvem um tempo de carregamento de perfil alto. Você pode:

- Redefinir o perfil do usuário
- Otimizar o perfil removendo arquivos grandes indesejados
- Reduzir o número de arquivos para diminuir a carga da rede
- Usar streaming de perfil

Por padrão, todos os nomes de pastas são visíveis. Para ocultar os nomes das pastas, edite os valores do registro na máquina VDA usando as seguintes etapas:

> **Aviso:**
>
> Adicionar e editar o registro incorretamente pode causar problemas sérios que podem exigir a reinstalação do seu sistema operacional. A Citrix não garante que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua própria conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

1. No VDA, adicione um novo valor de registro **ProfileFoldersNameHidden** em HKEY_LOCAL_MACHINE\Software\Citrix\Director\
2. Defina o valor como 1. Este valor deve ser um valor DWORD (32 bits). A visibilidade dos nomes das pastas agora está desativada.
3. Para tornar os nomes das pastas visíveis novamente, defina o valor como 0.

> **Nota:**

> Você pode usar GPO ou PowerShell para aplicar a alteração do valor do registro em várias máquinas. Para obter mais informações sobre como usar GPO para implantar alterações de registro, consulte o blog.

Informações adicionais

- A análise detalhada do perfil não considera pastas redirecionadas.
- Os arquivos NTUser.dat na pasta raiz podem não ser visíveis para os usuários finais. No entanto, eles são incluídos na análise detalhada do perfil e exibidos na lista de arquivos em **Root Folder**.
- Existem alguns arquivos ocultos na pasta AppData que não são incluídos na análise detalhada do perfil.
- O número de arquivos e os dados de tamanho do perfil podem não corresponder aos dados no painel de Personalização devido a certas limitações do Windows.

SESSÃO INTERATIVA

Este é o tempo levado para "entregar" o controle do teclado e mouse ao usuário após o carregamento do perfil do usuário. Normalmente, é a duração mais longa de todas as fases do processo de logon e é calculada como **duração da Sessão Interativa = Carimbo de Data/Hora do Evento Desktop Ready (EventId 1000 no VDA) - Carimbo de Data/Hora do Evento User Profile Loaded (EventId 2 no VDA)**. A Sessão Interativa possui três subfases: Pre-userinit, Userinit e Shell. Passe o mouse sobre a Sessão Interativa para ver uma dica de ferramenta mostrando o seguinte:

- subfases
- o tempo levado para cada subfase
- o atraso total de tempo cumulativo entre essas subfases

Você pode usar o botão recolhível para recolher ou expandir as opções na Sessão Interativa.

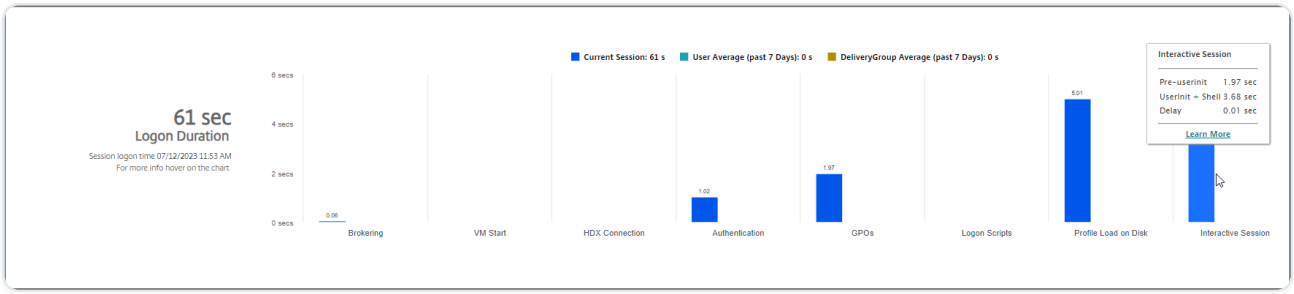
> **Observação:**

> Este recurso está disponível em VDAs 1811 e posteriores. Se você iniciou sessões em sites anteriores à versão 7.18 e depois atualizou para 7.18, uma mensagem de 'Detalhes indisponíveis devido a erro do servidor' é exibida. No entanto, se você iniciou sessões após uma atualização, nenhuma mensagem de erro é exibida.

> Para visualizar a duração de cada subfase, habilite o rastreamento de processo de auditoria (Audit process tracking) na VM (VDA). Quando o rastreamento de processo de auditoria está desabilitado (padrão), a duração de Pre-userinit e a duração combinada de Userinit e Shell são exibidas. Você pode habilitar o rastreamento de processo de auditoria por meio de um Objeto de Política de Grupo (GPO) da seguinte forma:

1. Crie um GPO e edite-o usando o editor de GPO.
2. Vá para **Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas Locais > Política de Auditoria**.
3. No painel direito, clique duas vezes em **Rastreamento de processo de auditoria**.
4. Selecione **Êxito** e clique em OK.
5. Aplique este GPO aos VDAs ou Grupo necessários.

Para obter mais informações sobre o rastreamento de processo de auditoria e como habilitá-lo ou desabilitá-lo, consulte `<https://docs.microsoft.com/pt-br/previous-versions/ms813609(v=msdn.10)>` na documentação da Microsoft.



Painel Duração de Logon na exibição Detalhes do Usuário.

- **Sessão Interativa – Pré-userinit:** Este é o segmento da Sessão Interativa que se sobrepõe aos Objetos de Política de Grupo e scripts. Esta subfase pode ser reduzida otimizando os GPOs e scripts.
- **Sessão Interativa – Userinit:** Quando um usuário faz logon em uma máquina Windows, o Winlogon executa userinit.exe. O Userinit.exe executa scripts de logon, restabelece conexões de rede e, em seguida, inicia o Explorer.exe, a interface do usuário do Windows. Esta subfase da Sessão Interativa representa a duração entre o início do Userinit.exe e o início da interface do usuário para o desktop virtual ou aplicativo.
- **Sessão Interativa – Shell:** Na fase anterior, o Userinit inicia a inicialização da interface do usuário do Windows. A subfase Shell captura a duração entre a inicialização da interface do usuário e o momento em que o usuário recebe o controle do teclado e do mouse.

- **Atraso:** Este é o atraso de tempo cumulativo entre as subfases **Pré-userinit e Userinit** e as subfases **Userinit e Shell**.

O tempo total de logon não é a soma exata dessas fases. Por exemplo, algumas fases ocorrem em paralelo e, em algumas fases, ocorre processamento extra que pode resultar em uma duração de logon mais longa do que a soma. O tempo total de logon não inclui o tempo ocioso do ICA®, que é o tempo entre o download do arquivo ICA e o lançamento do arquivo ICA para um aplicativo. Para habilitar a abertura automática do arquivo ICA no lançamento do aplicativo, configure seu navegador para o lançamento automático do arquivo ICA após o download de um arquivo ICA. Para obter mais informações, consulte CTX804493.

> **Nota:**
>
> O gráfico Duração de Logon mostra as fases de logon em segundos. Quaisquer valores de duração abaixo de um segundo são exibidos como valores de subsegundo. Os valores acima de um segundo são arredondados para o 0,5 segundo mais próximo. O gráfico foi projetado para mostrar o valor mais alto do eixo y como 200 segundos. Qualquer valor maior que 200 segundos é mostrado com o valor real exibido acima da barra.

Scripts de logon
Se os scripts de logon estiverem configurados para a sessão, este é o tempo necessário para que os scripts de logon sejam executados.
GPOs
Se as configurações de Política de Grupo estiverem habilitadas nas máquinas virtuais, este é o tempo necessário para aplicar os objetos de política de grupo durante o logon. O detalhamento do tempo necessário para aplicar cada política de acordo com as CSEs (Extensão do Lado do Cliente) está disponível como uma dica de ferramenta ao passar o mouse sobre a barra GPO.



Clique em **Detalhes** para ver uma tabela com o status da política e o nome GPO correspondente. As durações de tempo no detalhamento representam apenas o tempo de processamento do CSE e não somam o tempo total do GPO. Você pode copiar a tabela de detalhamento para solução de problemas adicionais ou uso em relatórios. O tempo GPO para as políticas é recuperado dos logs do Visualizador de Eventos. Os logs podem ser sobrescritos dependendo da memória alocada para os logs operacionais (o tamanho padrão é 4 MB). Para obter mais informações sobre como aumentar o tamanho do log para os logs operacionais, consulte o artigo do Microsoft TechNet Configuring the Event Logs.

Início do usuário

Quando um usuário faz logon em uma máquina Windows, o Winlogon executa userinit.exe. O Userinit.exe executa scripts de logon, restabelece conexões de rede e, em seguida, inicia o Explorer.exe, a interface do usuário do Windows. Esta subfase da Sessão Interativa representa a duração entre o início do Userinit.exe e o início da interface do usuário para o desktop virtual ou aplicativo.

SHELL

A subfase Shell captura a duração entre a inicialização da interface do usuário e o momento em que o usuário recebe o controle do teclado e do mouse.

Associações de arquivos AppX

O tempo levado para associar arquivos AppX durante a nova sessão VDA.

Carregamento de pacotes AppX

O tempo levado para carregar os pacotes AppX durante a nova sessão VDA.

> **Nota:**

> O uberAgent deve ser integrado ao Monitor para coletar a duração do carregamento dos pacotes AppX durante a nova sessão VDA. Para esta integração, instale o VDA e, em seguida, configure o uberAgent via políticas Citrix.

EXPORTAR DADOS

Juntamente com as opções padrão da tabela Fases de Duração de Logon, que são Fase de Logon da Sessão e Duração, você também pode escolher as seguintes colunas na página Logon da Sessão:

- Hora de início
- Hora de término
- Grupo de Entrega - Média de 7d (seg)
- Usuário - Média de 7d (seg)

Você também pode exportar os dados precedentes para um arquivo .CSV.

Dicas de solução de problemas

Para identificar valores incomuns ou inesperados no gráfico, compare a quantidade de tempo gasto em cada fase da sessão atual com a duração média para este usuário nos últimos sete dias e a duração média para todos os usuários neste grupo de entrega nos últimos sete dias.

Escalone conforme necessário. Por exemplo, se a **Inicialização da Máquina** estiver lenta, o problema pode estar no hipervisor, então você pode escalá-lo para o administrador do hipervisor. Ou, se o tempo de corretagem estiver lento, você pode escalar o problema para o administrador do site para verificar o balanceamento de carga no Delivery Controller.

Examine as diferenças incomuns, incluindo:

- Barras de logon (atuais) ausentes
- Grande discrepância entre a duração atual e a duração média deste usuário. As causas incluem:
  - Uma nova aplicação foi instalada.
  - Uma atualização do sistema operacional ocorreu.
  - Alterações de configuração foram feitas.
  - O tamanho do perfil do usuário é alto. Neste caso, a Carga do Perfil é alta.

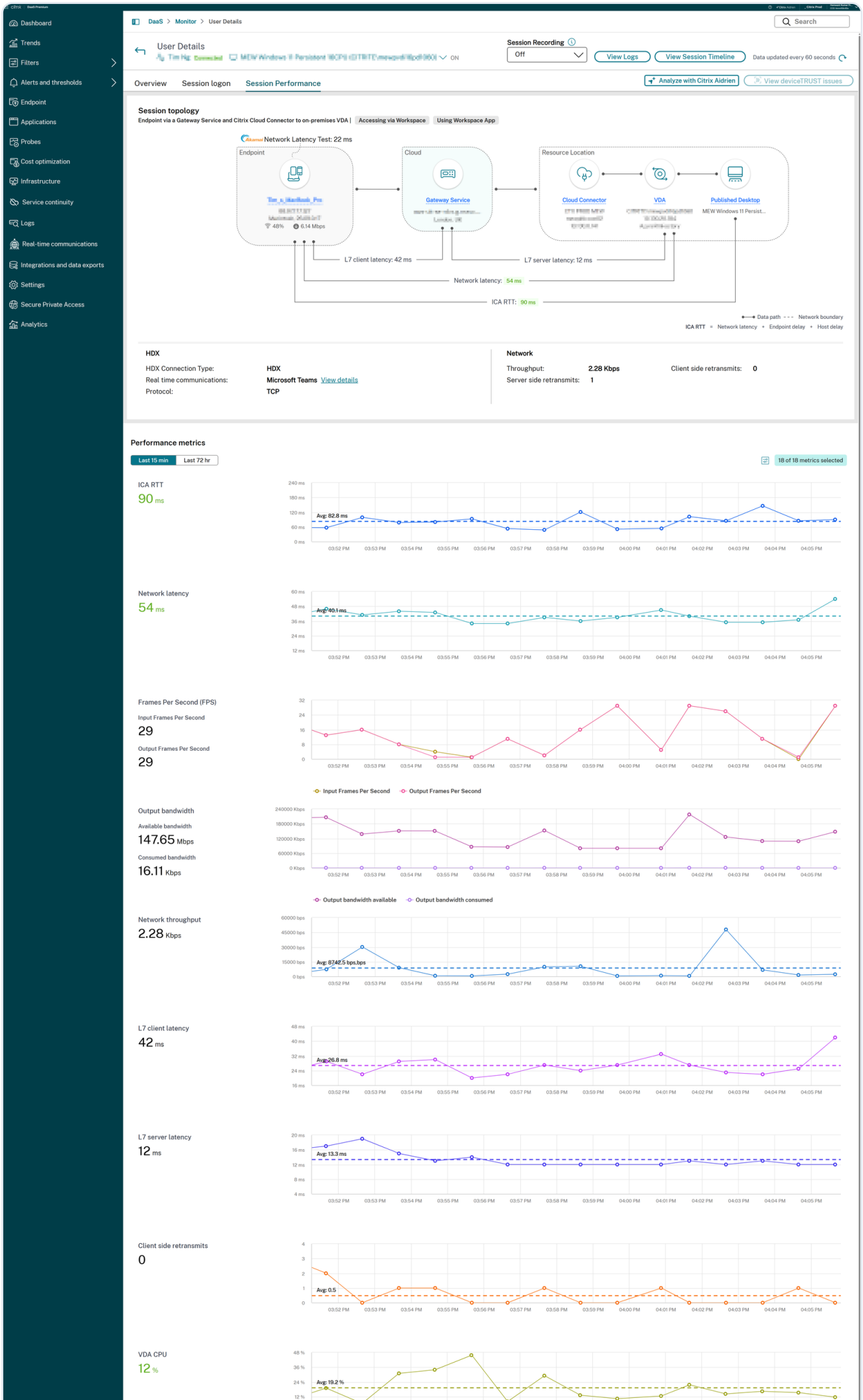
- Grande discrepância entre os números de logon do usuário (duração atual e média) e a duração média do grupo de entrega.

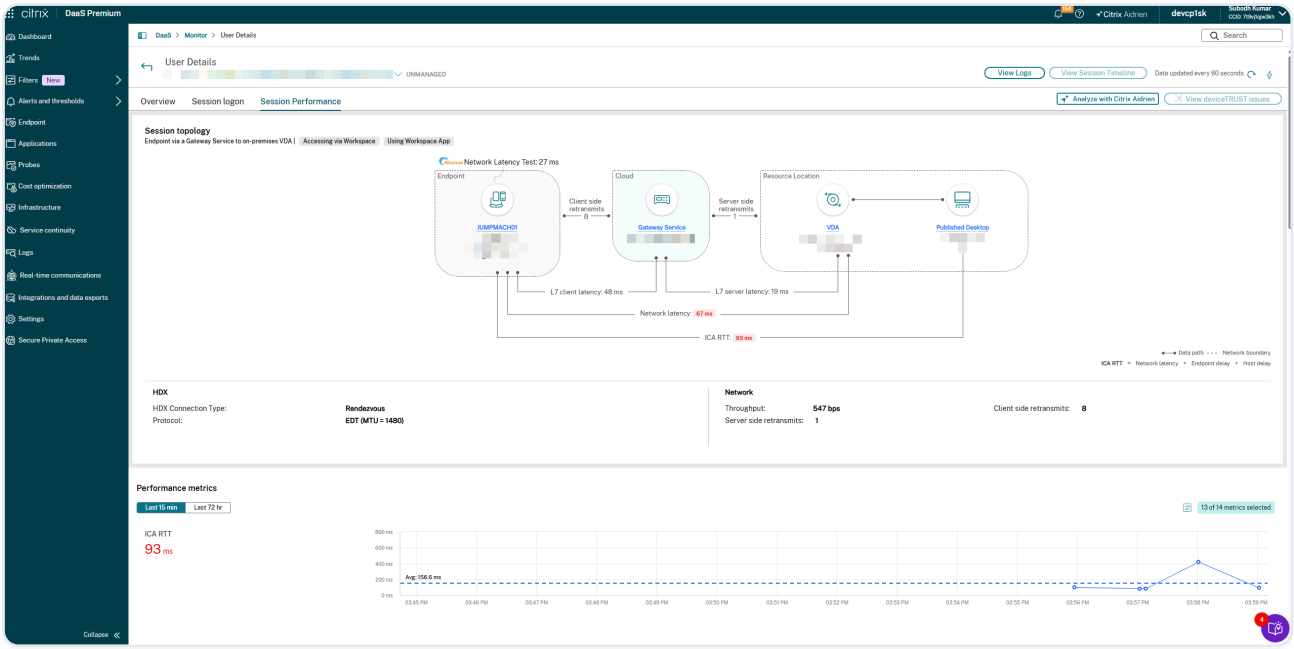
Se necessário, clique em **Reiniciar** para observar o processo de logon do usuário e solucionar problemas, como Inicialização da Máquina ou Corretagem.

Diagnosticar problemas de desempenho da sessão

A guia **Desempenho da Sessão** na Página de Detalhes do Usuário possui fluxos de trabalho de solução de problemas aprimorados para ajudar a identificar problemas em sessões de usuário HDX™. Os painéis **Topologia da Sessão e Métricas de Desempenho** ajudam a correlacionar a visualização de componentes e múltiplas métricas de desempenho de uma sessão em uma única visualização e reduzem o tempo médio para a resolução de problemas de experiência da sessão.

CITRIX DAAS™


Dashboard
Trends
Filters
Alerts and thresholds
Endpoint
Applications
Probes
Cost optimization
Infrastructure
Service continuity
Logs
Real-time communications
Integrations and data exports
Settings
Secure Private Access
Analytics
DaaS > Monitor > User Details
Search
User Details
Session Recording
Off
View Logs
View Session Timeline
Data updated every 60 seconds
Overview
Session logon
Session Performance
Analyze with Citrix Aidrien
View deviceTRUST issues
Session topology
Endpoint via a Gateway Service and Citrix Cloud Connector to on-premises VDA |
Accessing via Workspace
Using Workspace App
Network Latency Test: 22 ms
Endpoint
Cloud
Resource Location
Gateway Service
Cloud Connector
VDA
Published Desktop
MEW Windows 11 Persist...
6.14 Mbps
L7 client latency: 42 ms
L7 server latency: 12 ms
Network latency: 54 ms
ICA RTT: 90 ms
Data path
Network boundary
ICA RTT = Network latency + Endpoint delay + Host delay
HDX
HDX Connection Type: HDX
Real time communications: Microsoft Teams View details
Protocol: TCP
Network
Throughput: 2.28 Kbps
Server side retransmits: 1
Client side retransmits: 0
Performance metrics
Last 15 min
Last 72 hr
18 of 18 metrics selected
ICA RTT
90 ms
Avg: 82.8 ms
Network latency
54 ms
Avg: 40.1 ms
Frames Per Second (FPS)
Input Frames Per Second
29
Output Frames Per Second
29
Input Frames Per Second
Output Frames Per Second
Output bandwidth
Available bandwidth
147.65 Mbps
Consumed bandwidth
16.11 Kbps
Output bandwidth available
Output bandwidth consumed
Network throughput
2.28 Kbps
Avg: 8742.5 bps,bps
L7 client latency
42 ms
Avg: 26.8 ms
L7 server latency
12 ms
Avg: 13.3 ms
Client side retransmits
0
Avg: 0.5
VDA CPU
12 %
Avg: 19.2 %



Visualização de Salto de Rede de Ponta a Ponta

A visualização de salto de rede de ponta a ponta oferece uma representação visual do caminho completo da sessão, auxiliando significativamente na solução de problemas. Você pode acessar esta visualização em **Detalhes do Usuário** > **Desempenho da Sessão** > **Topologia da Sessão**. A visualização de salto de rede de ponta a ponta exibe componentes, metadados, links e aplicativos publicados para sessões HDX conectadas.

Esta visualização ajuda os administradores a:

- Compreender o fluxo de dados da sessão.
- Identificar gargalos de desempenho em saltos específicos.

MÉTRICAS DE DESEMPENHO DA SESSÃO

As seguintes métricas estão disponíveis contextualmente para ajudar os administradores a entender o desempenho da sessão fornecida. As métricas apresentadas na visualização de salto de rede de ponta a ponta estão disponíveis em tempo quase real e são atualizadas periodicamente com base nos intervalos mostrados na interface do usuário.

Métricas de Endpoint

As métricas de endpoint são vitais para a solução de problemas de desempenho da sessão Citrix®, pois fornecem insights sobre a "última milha" da experiência do usuário e revelam detalhes sobre o ambiente imediato do usuário. Essas métricas ajudam a identificar gargalos locais, como Wi-Fi ruim, baixa taxa de transferência de rede, limitações de dispositivos de endpoint, distinguindo entre problemas do lado do servidor e do lado do cliente. Ao oferecer uma visão holística quando combinados com métricas na topologia da sessão, os dados de endpoint

permitem uma identificação mais rápida da causa raiz e uma resolução mais ágil dos problemas de desempenho, melhorando a experiência do usuário.

Use as políticas no Citrix Studio para habilitar ou desabilitar a coleta das métricas de endpoint listadas com base em seus requisitos. As políticas fornecem aos administradores Citrix controles granulares para relatar métricas em conformidade com seus requisitos de conformidade.

NOME DA POLÍTICA	DESCRIÇÃO DA POLÍTICA	MÉTRICAS DA UI	VALOR PADRÃO	OPÇÕES DE VALOR	VERSÃO DO VDA PARA WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA PARA LINUX
Intervalo de estatísticas do endpoint	Permite a coleta de detalhes da rede do endpoint a partir do endpoint do usuário. Habilitar esta política é um pré-requisito para que outras políticas relacionadas ao endpoint entrem em vigor.	Força do sinal Wi-Fi, Tipo de interface de rede, Taxa de transferência de entrada ou saída, Velocidade do link, Tipo de Workspace, CPU do endpoint, Memória do endpoint, GPU do	Habilitado	Habilitado ou Desabilitado. Opção para modificar a frequência entre 60s - 3600s. 60s é o valor sugerido	2407 ou posterior	2607	2607

NOME DA POLÍTICA	DESCRIÇÃO DA POLÍTICA	MÉTRICAS DA UI	VALOR PADRÃO	OPÇÕES DE VALOR	VERSÃO DO VDA PARA WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA PARA LINUX
		endpoint					
Coleta de dados de localização do endpoint	Permite a coleta de detalhes de localização do endpoint e do ISP a partir do endpoint do usuário usando o serviço Locus - `<https://locus.analytics.cloud.com>`	Endereço IP público, País, Cidade e Provedor de Serviços de Internet.	Desabilitado	Habilitado ou Desabilitado	2411 ou posterior	2607	2607
Intervalo de medição da latência da rede do	Permite a medição e coleta da latência da rede	Latência da rede (em Detalhes da rede do	Desabilitado	Habilitado ou Desabilitado. Opção para modificar a	2411 ou posterior	2607	2607

NOME DA POLÍTICA	DESCRIÇÃO DA POLÍTICA	MÉTRICAS DA UI	VALOR PADRÃO	OPÇÕES DE VALOR	VERSÃO DO VDA PARA WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA PARA LINUX
endpoint	entre o endpoint e o host beacon - `<https://downloadplugins.citrix.com>`	endpoint)		frequência entre 60s - 3600s. 60s é o valor sugerido.			

Nota:

A partir do Citrix Virtual Apps and Desktops™ 2507 ou posterior, a política de **coleta de dados de localização do endpoint** e a política de **intervalo de medição de latência de rede do endpoint** estão desabilitadas por padrão. Consequentemente, os dados relacionados não estão disponíveis no Director, a menos que essas políticas sejam habilitadas manualmente no Studio.

As métricas de endpoint que estão prontamente disponíveis estão listadas abaixo:

- Nome do endpoint
- IP do endpoint
- SO do endpoint
- Versão do aplicativo Citrix Workspace™

A tabela a seguir lista as métricas dependentes das versões de produtos suportadas:

NOME DO RECURSO	PARÂMETROS DE UI	VERSÃO DO VDA PARA WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROME OS
Detalhes da rede do endpoint	Tipo de interface de rede	2407 ou posterior	NA	NA	2405.10 ou posterior	2409 ou posterior	2408 ou posterior	2411 ou posterior	2411 ou posterior
	Força do sinal	2407 ou posterior	NA	NA	2405.10 ou posterior	2409 ou posterior	2408 ou posterior	Não aplicável	Não aplicável
	Taxa de transferência do endpoint (entrada, saída)	2407 ou posterior	NA	NA	2405.10 ou posterior	2409 ou posterior	2408 ou posterior	Não aplicável	Não aplicável
	Velocidade	2407 ou	NA	NA	2405.10 ou	2409 ou	2408 ou	2411 ou	2411 ou

NOME DO RECURSO	PARÂMETROS DE UI	VERSÃO DO VDA PARA WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROMEOS
	do link	posterior			posterior	posterior	posterior	posterior	posterior
	Endereço IP público do endpoint	2411 ou posterior	NA	NA	2409 ou posterior	2409 ou posterior	2408 ou posterior	2411 ou posterior	2411 ou posterior
	Cidade do endpoint, País do endpoint	2411 ou posterior	NA	NA	2409 ou posterior	2409 ou posterior	2408 ou posterior	2411 ou posterior	2411 ou posterior
	Provedor de serviços de	2411 ou posterior	NA	NA	2409 ou posterior	2409 ou posterior	2408 ou posterior	2411 ou posterior	2411 ou posterior

NOME DO RECURSO	PARÂMETROS DE UI	VERSÃO DO VDA PARA WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROME OS
	internet								
	Tipo de Workspace	2411 ou posterior	NA	NA	2409 ou posterior	2409 ou posterior	2408 ou posterior	2411 ou posterior	2411 ou posterior
	Tipo de acesso (via Workspace / StoreFront)	2411 ou posterior	NA	NA	2409 ou posterior	2409 ou posterior	2408 ou posterior	2411 ou posterior	2411 ou posterior
	CPU do Endpoint	2411 ou posterior	NA	NA	2409 ou posterior	2409 ou posterior	2408 ou posterior	Não aplicável	2411 ou posterior

NOME DO RECURSO	PARÂMETROS DE UI	VERSÃO DO VDA PARA WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROME OS
	Memória do endpoint	2411 ou posterior	NA	NA	2409 ou posterior	2409 ou posterior	2408 ou posterior	Não aplicável	2411 ou posterior
	GPU do endpoint	2411 ou posterior	NA	NA	2409 ou posterior	2409 ou posterior	2408 ou posterior	Não aplicável	Não aplicável
	Latência da rede	2411 ou posterior	NA	NA	2409 ou posterior	2409 ou posterior	2408 ou posterior	2411 ou posterior	2411 ou posterior

Definições de dados:

PARÂMETRO DA IU	DESCRIÇÃO
Nome do endpoint	Nome do dispositivo endpoint do usuário usado para a sessão.
IP do endpoint	Endereço IP do endpoint conforme disponível para o Virtual Delivery Agent (VDA). Pode

PARÂMETRO DA IU	DESCRIÇÃO
	conter endereços IP privados ou públicos do dispositivo endpoint.
SO do endpoint	Sistema operacional do dispositivo endpoint
Versão do Citrix Workspace App	Versão do aplicativo Citrix Workspace instalada
Força do sinal	Exibe a qualidade e a força do sinal sem fio.
Vazão do endpoint (entrada, saída)	Indica a taxa de transferência de dados para dentro e para fora da interface de rede. Análogo à velocidade de upload e download da internet observada no endpoint.
Velocidade do link	Especifica o tipo de conexão de rede, como Ethernet, Wi-Fi ou celular.
Tipo de interface de rede	Representa a taxa máxima de transferência de dados da conexão de rede.
Endereço IP público do endpoint	O endereço IP externo atribuído ao seu dispositivo pelo seu provedor de serviços de internet.
Cidade do endpoint, País do endpoint	A localização geográfica, incluindo país e cidade, do dispositivo.
Provedor de serviços de internet	O nome da empresa que fornece acesso à internet ao dispositivo do usuário final.
Tipo de workspace	O tipo de workspace em uso, seja o aplicativo Citrix Workspace ou um navegador da web.
Tipo de acesso (via Workspace / StoreFront)	O método de acesso aos recursos, seja por meio do Citrix® StoreFront Cloud (anteriormente conhecido como Citrix Workspace) ou do StoreFront local.
CPU do endpoint	A porcentagem de recursos de CPU atualmente em uso.

PARÂMETRO DA IU	DESCRIÇÃO
Memória do endpoint	A porcentagem de recursos de memória atualmente em uso.
GPU do endpoint	A porcentagem de recursos de GPU atualmente em uso.
Teste de latência de rede	O atraso de tempo experimentado na rede, medido em milissegundos.

Métricas de rede

As métricas de rede são críticas para a solução de problemas de sessão do Citrix porque o desempenho e a estabilidade de uma sessão do Citrix dependem muito das condições da rede subjacente. Ao contrário de um aplicativo local, uma sessão do Citrix envolve o streaming de uma experiência interativa de desktop ou aplicativo por uma rede, o que significa que qualquer instabilidade ou gargalo na rede impactará diretamente a percepção de desempenho do usuário.

A coleta de métricas de rede pode ser ativada ou desativada por meio de políticas Citrix no Citrix Studio. Para obter informações adicionais sobre os requisitos para métricas de rede, consulte Telemetria de rede.

NOME DA CONFIGURAÇÃO	DESCRIÇÃO DA POLÍTICA	MÉTRICAS DE IU	VALOR PADRÃO	OPÇÕES DE VALOR	VERSÃO DO VIRTUAL DELIVERY AGENT
Telemetria de rede	Permite a coleta de detalhes de rede entre o endpoint do usuário e os componentes de back-end.	Todas as métricas de insights HDX para Citrix Gateway e serviço Citrix Gateway	Desativado	Ativado ou Desativado.	2411 ou posterior para o serviço Gateway. 2503 ou posterior para Citrix Gateway

Serviço Citrix Gateway

A tabela a seguir lista as métricas dependentes das versões de produto suportadas:

NOME DO RECURSO	PARÂMETROS DA UI	VERSÃO DO VDA PARA WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROMEOS
Métricas de rede	Latência do servidor L7	2411 ou superior	2507 ou posterior	2507 ou posterior	2409 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607
	Latência do cliente L7	2411 ou superior	2507 ou posterior	2507 ou posterior	2409 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607
	Retransmissões do lado do cliente Observação: Disponível apen	2411 ou superior	2507 ou posterior	2507 ou posterior	2409 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607

NOME DO RECURSO	PARÂMETROS DA UI	VERSÃO DO VDA PARA WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROME OS
	as para sessões TCP								
	Taxa de transferência	2411 ou superior	NA	NA	2409 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607

Citrix Gateway

A tabela a seguir lista as métricas dependentes das versões de produto suportadas:

NOME DO RECURSO	PARÂMETROS DE IU	VERSÃO DO CITRIX GATEWAY	VERSÃO DO VDA PARA WINDOWS	VERSÃO PARA MAC	VERSÃO PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROMEOS
Métricas de rede	Latência da WAN	Netscaler 14.1-47.46 ou superior	2503 ou posterior	2507 ou posterior	2507 ou posterior	2503 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607
	Latência do DC	Netscaler 14.1-47.46 ou superior	2503 ou posterior	2507 ou posterior	2507 ou posterior	2503 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607
	Retransmissões do	Netscaler 14.1-47.	2503 ou posterior	2507 ou posterior	2507 ou posterior	2503 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607

NOME DO RECURSO	PARÂMETROS DE IU	VERSÃO DO CITRIX GATEWAY	VERSÃO DO VDA PARA WINDOWS	VERSÃO PARA MAC	VERSÃO PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROMEOS
	Lado do Servidor	46 ou superior								
	Retransmissões do Lado do Cliente	Netscaler 14.1-47.46 ou superior	2503 ou posterior	2507 ou posterior	2507 ou posterior	2503 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607
	Latência do servidor L7	Netscaler 14.1-47.46 ou superior	2503 ou posterior	2507 ou posterior	2507 ou posterior	2503 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607

NOME DO RECURSO	PARÂMETROS DE IU	VERSÃO DO CITRIX GATEWAY	VERSÃO DO VDA PARA WINDOWS	VERSÃO PARA MAC	VERSÃO PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROMEOS
	Latência do cliente L7	Netscaler 14.1-47.46 ou superior	2503 ou posterior	2507 ou posterior	2507 ou posterior	2503 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607
	Evento de tamanho de janela zero do lado do cliente	Netscaler 14.1-47.46 ou superior	2503 ou posterior	2507 ou posterior	2507 ou posterior	2503 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607

NOME DO RECURSO	PARÂMETROS DE IU	VERSÃO DO CITRIX GATEWAY	VERSÃO DO VDA PARA WINDOWS	VERSÃO PARA MAC	VERSÃO PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROMEOS
	RTO rápido do lado do cliente	Netscaler 14.1-47.46 ou superior	2503 ou posterior	2507 ou posterior	2507 ou posterior	2503 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607
	Evento de tamanho de janela zero do lado do servidor	Netscaler 14.1-47.46 ou superior	2503 ou posterior	2507 ou posterior	2507 ou posterior	2503 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607

NOME DO RECURSO	PARÂMETROS DE IU	VERSÃO DO CITRIX GATEWAY	VERSÃO DO VDA PARA WINDOWS	VERSÃO PARA MAC	VERSÃO PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROMEOS
	RTO rápido do lado do servidor	Netscaler 14.1-47.46 ou superior	2503 ou posterior	2507 ou posterior	2507 ou posterior	2503 ou posterior	2505 ou posterior	2505 ou posterior	2607	2607

Definições de dados:

PARÂMETRO DE UI	DESCRIÇÃO
Latência da WAN	Latência causada pelo lado do cliente da rede, do NetScaler® ao usuário final.
Latência do DC	Latência causada pelo lado do servidor da rede, do NetScaler aos servidores de backend.
Latência do Cliente L7	A latência L7 média observada entre o cliente ICA® e a instância do NetScaler. Essa métrica é útil em dispositivos não-Citrix que estão presentes no caminho de entrega.

PARÂMETRO DE UI	DESCRIÇÃO
Latência do Servidor L7	A latência L7 média observada entre o dispositivo NetScaler e o Citrix Virtual App. Essa métrica é útil quando dispositivos não-Citrix estão presentes no caminho de entrega.
Retransmissões do cliente	O número de pacotes retransmitidos na conexão entre o NetScaler e o usuário final. Um valor alto desta métrica indica alta utilização da largura de banda devido a retransmissões, mas não significa necessariamente uma experiência de usuário ruim. Nota: Para sessões que usam o serviço Gateway, as retransmissões do cliente estão disponíveis apenas para sessões TCP.
Retransmissões do lado do servidor	O número de pacotes retransmitidos na conexão entre o NetScaler e o servidor de back-end.
Contagem de janela zero do lado do cliente	O número de vezes que o cliente anunciou uma janela TCP zero.
Contagem de janela zero do lado do servidor	O número de vezes que o servidor anunciou uma janela TCP zero.

Métricas HDX

As métricas HDX são fundamentais para entender e solucionar problemas de qualidade da experiência virtual do usuário. Essas métricas medem diretamente o desempenho do protocolo ICA/HDX que entrega a sessão virtual.

> **Nota:**
>
> As métricas ICA estão disponíveis a partir do Citrix Workspace app para Windows versão 2405.10 ou posterior, e Citrix Virtual Apps and Desktops 2407 ou posterior. No entanto, atualizações e correções para os dados estão disponíveis em versões recentes. Consulte a tabela a seguir para as versões recomendadas para cada ponto de dados:

NOME DO RECURSO	PARÂMETROS DA UI	VERSÃO DO VDA DO WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5
Métricas ICA	RTT ICA	2507 ou posterior	NA	NA	2503 ou posterior	2503 ou posterior	2503 ou posterior	2503 ou posterior
	Latência da rede	2507 ou posterior	NA	NA	2503 ou posterior	2503 ou posterior	2503 ou posterior	2503 ou posterior
	Tipo de conexão HDX	2411 ou posterior	NA	NA	2411 ou posterior	2411 ou posterior	2411 ou posterior	2411 ou posterior
	Protocolo	2411 ou posterior	NA	NA	2411 ou posterior	2411 ou posterior	2411 ou posterior	2411 ou posterior
	EDT MTU	2411 ou posterior	NA	NA	2411 ou posterior	2411 ou posterior	2411 ou posterior	2411 ou posterior

Definições de dados:

PARÂMETRO DE UI	DESCRIÇÃO
ICA RTT	Mede o tempo entre a ação do usuário e a resposta da tela. O contador Thinwire RTT representa essa métrica a partir da versão 2507 do Citrix Virtual Apps and Desktops. As versões anteriores continuam a usar o EUEM RTT.
Latência da rede	Indica latência da rede e possível lentidão. Definido como a soma da latência do lado do cliente e do servidor a partir da versão 2503 do Citrix Virtual Apps and Desktops. As versões anteriores continuam a usar a latência HDX relatada no VDA.
Tipo de conexão HDX	Tipo de conexão HDX para a sessão do usuário.
Protocolo	Protocolo subjacente usado para a sessão do usuário. Os valores podem ser *TCP* ou *EDT*.
EDT MTU	MTU, referida como Unidade Máxima de Transmissão, é o maior tamanho de um pacote (em bytes) que uma interface de rede pode enviar sem precisar fragmentá-lo. O MTU EDT representa o MTU estabelecido para a sessão EDT do usuário.

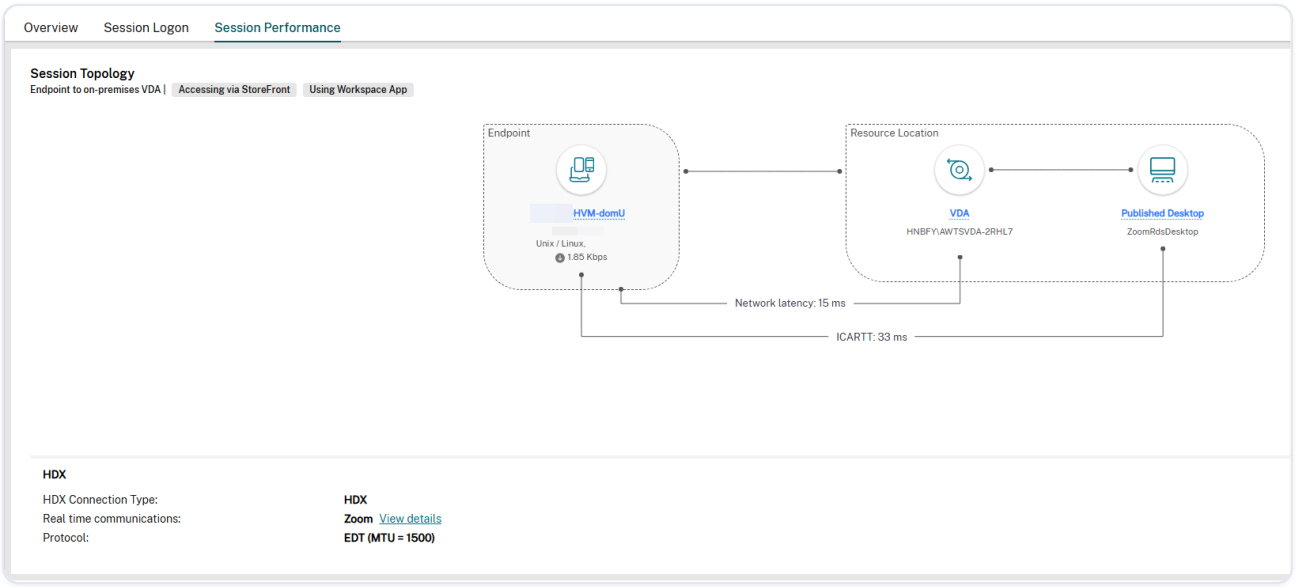
Visibilidade da otimização de comunicações em tempo real
A topologia da sessão oferece visibilidade abrangente sobre o status de otimização de aplicativos de comunicação em tempo real (RTC), como Microsoft Teams, Zoom e WebEx, dentro das sessões Citrix. Ela identifica se um aplicativo está otimizado e aponta quaisquer componentes ausentes (como plug-ins necessários, gerenciamento de plug-ins ou limitações específicas da plataforma) que impedem o desempenho ideal.

Benefícios:

- Os clientes obtêm garantia clara sobre a otimização de aplicativos RTC, eliminando suposições sobre se uma sessão está realmente otimizada.

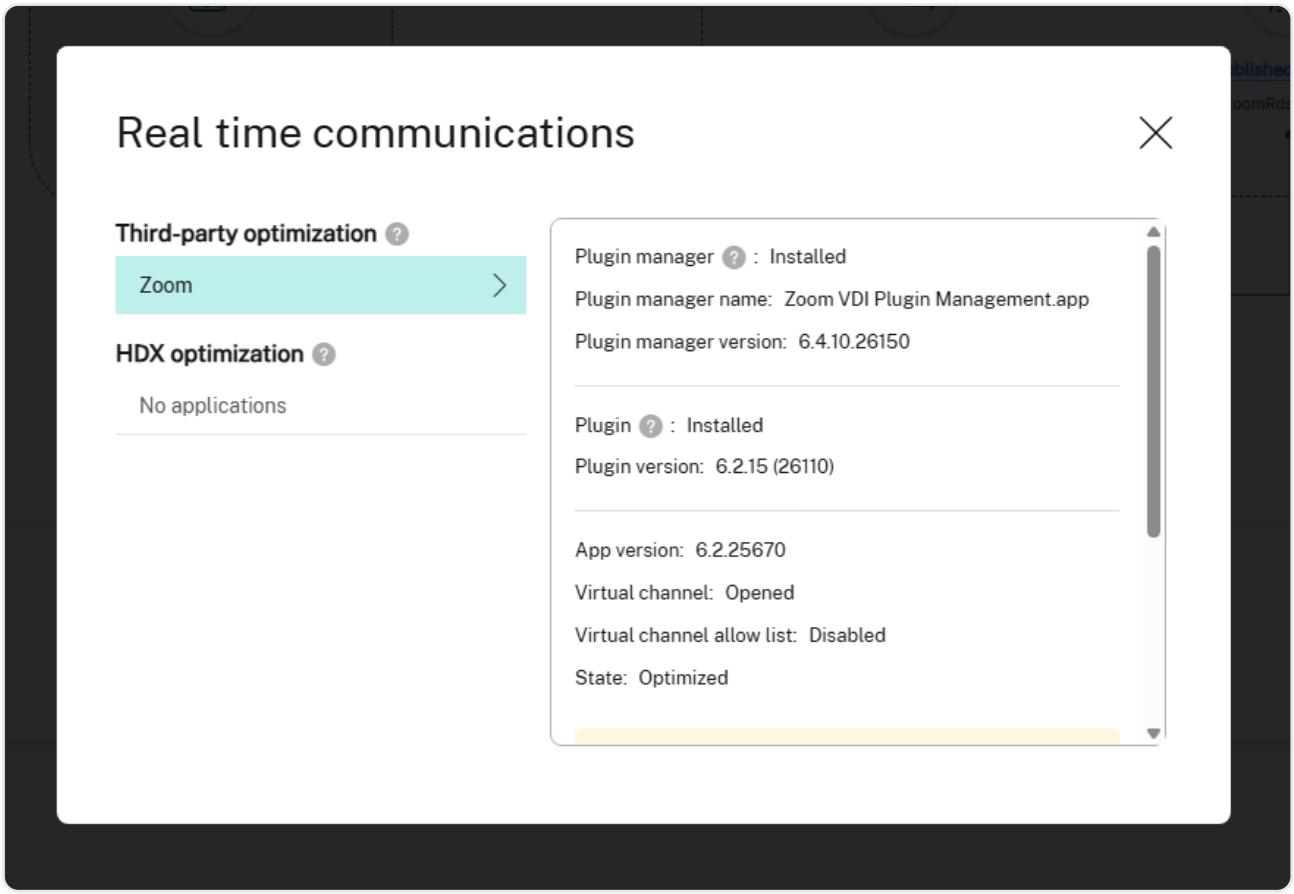
- Visão direta sobre componentes ausentes para resolver proativamente os problemas e alcançar a otimização completa.
- A solução de problemas mais rápida melhora a experiência do usuário para ferramentas de comunicação importantes.

Use o campo **Comunicações em tempo real** em **Topologia da Sessão** para visualizar os detalhes de otimização de cada aplicativo.



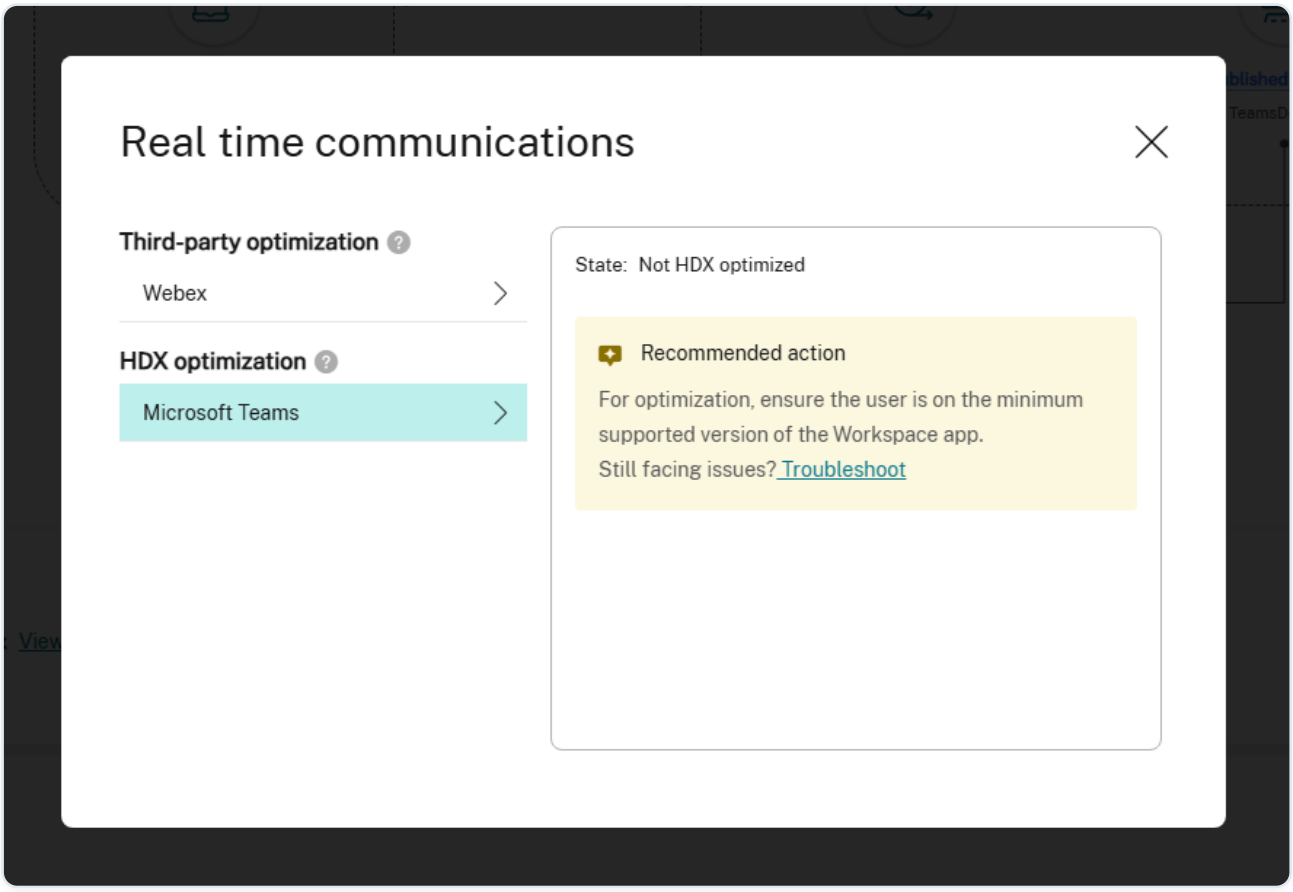
Aplicativos otimizados de terceiros criam um canal virtual usando a tecnologia Citrix, mas o fornecedor do aplicativo gerencia outras configurações e ajustes. A otimização depende de soluções de propriedade do fornecedor.

Clique no link **Ver detalhes** ao lado do campo **Comunicações em tempo real** na tela **Topologia da Sessão**. A seguinte tela aparece:



Aplicativos otimizados para HDX usam o canal virtual Citrix e são diretamente impactados pelas configurações e definições do Citrix.

Clique na seção **Otimização HDX** na tela **Comunicações em tempo real**. A imagem a seguir aparece:



Os detalhes das comunicações em tempo real são atualizados a cada 5 minutos. A tabela a seguir lista os detalhes disponíveis para um aplicativo que depende de otimização de terceiros. Certifique-se de que você está usando versões de produto compatíveis para obter visibilidade total.

Nota:

- A otimização do Microsoft Teams Slimcore está disponível apenas para desktops publicados e para o New Teams, conforme o suporte do fornecedor.
- Para o Zoom, as alterações do fornecedor para buscar detalhes do plug-in e estados de otimização estão disponíveis a partir da versão 6.3.10. Para mais informações, consulte a documentação do Zoom.

A tabela a seguir lista os detalhes disponíveis para um aplicativo que depende da otimização Citrix HDX. Certifique-se de que você está usando versões de produto compatíveis para obter visibilidade total.

NOME DO RECURSO	PARÂMETROS DE UI	VERSÃO DO VIRTUAL DELIVERY AGENT	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX
Microsoft Teams Slimcore	Gerenciador de plug-ins, Nome do gerenciador de plug-ins, Versão do gerenciador de plug-ins	2503	2503	Não suportado pelo fornecedor	Não suportado pelo fornecedor
	Versão do aplicativo, Canal virtual, Lista de permissões de canal virtual	2503	2402	Não suportado pelo fornecedor	Não suportado pelo fornecedor
	Plug-in, Versão do plug-in, Estado	2507	2503	Não suportado pelo fornecedor	Não suportado pelo fornecedor
Zoom	Gerenciador de plug-ins, Nome do gerenciador de plug-ins, Versão do gerenciador de plug-ins	2507	2503	2505	Plug-in não disponível
	Versão do aplicativo, Canal virtual, Lista	2507	2402	2402	2402

NOME DO RECURSO	PARÂMETROS DE UI	VERSÃO DO VIRTUAL DELIVERY AGENT	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX
	de permissões do canal virtual				
	Plugin, Versão do Plugin, Estado	2507	2503	2505	Plugin Não Disponível
Webex	Gerenciador de plugins, Nome do gerenciador de plugins, Versão do gerenciador de plugins	2507	2503	Plugin Não Disponível	Plugin Não Disponível
	Versão do aplicativo, Canal virtual, Lista de permissões do canal virtual	2507	2402	2402	2402

A tabela a seguir lista os detalhes disponíveis para um aplicativo que depende da otimização do Citrix HDX. Certifique-se de que você está usando versões de produto compatíveis para obter visibilidade total.

NOME DO RECURSO	PARÂMETROS DE UI	VERSÃO DO VIRTUAL DELIVERY AGENT	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA WINDOWS	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX
Microsoft Teams	Estado	1906.2	2112	2203	2203

Definições de dados:

PARÂMETRO UI	DESCRIÇÃO
Gerenciador de plug-ins	Mostra se o gerenciador de plug-ins está instalado ou não. O gerenciador de plug-ins é um pequeno componente de gerenciamento que abre o canal virtual e baixa o mecanismo de mídia (plug-in) necessário para otimização. Observação: A funcionalidade pode variar de acordo com o fornecedor.
Nome do gerenciador de plug-ins	Nome do gerenciador de plug-ins instalado.
Versão do gerenciador de plug-ins	Versão do gerenciador de plug-ins instalado.
Plug-in	Mostra se o plug-in está instalado ou não. O plug-in é o mecanismo de mídia necessário para otimização. Observação: A funcionalidade pode variar de acordo com o fornecedor.
Versão do plug-in	Versão do plug-in instalado no endpoint.
Versão do aplicativo	Representa a versão do aplicativo no agente de entrega virtual (VDA).
Canal virtual	Representa se o canal virtual está aberto ou fechado para o aplicativo de comunicações em tempo real.
Lista de permissões de canal virtual	Mostra o status dos canais virtuais. Os valores são *Habilitado* ou *Desabilitado*.

PARÂMETRO UI	DESCRIÇÃO
Estado	Mostra o estado de otimização para o aplicativo para a sessão de usuário específica

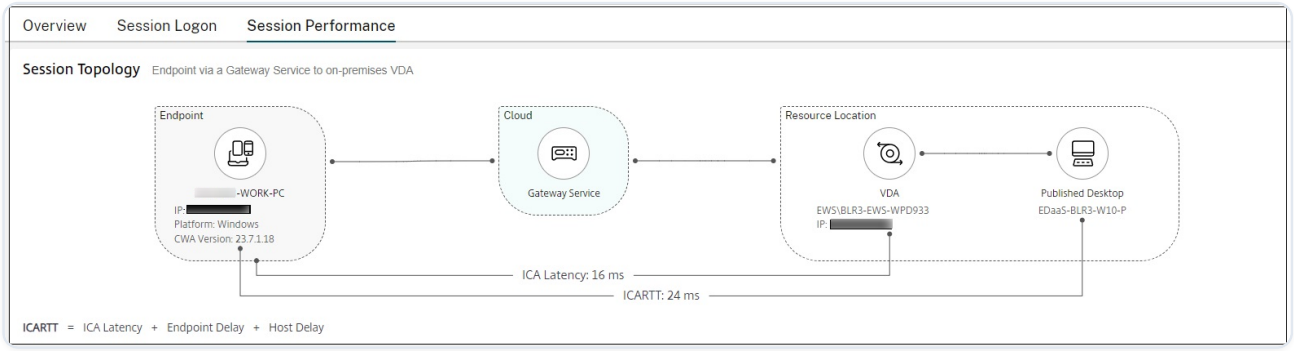
CENÁRIOS DE TOPOLOGIA DE SESSÃO

Dependendo do cenário de implantação do site, os componentes envolvidos em uma sessão são todos ou qualquer um dos seguintes:

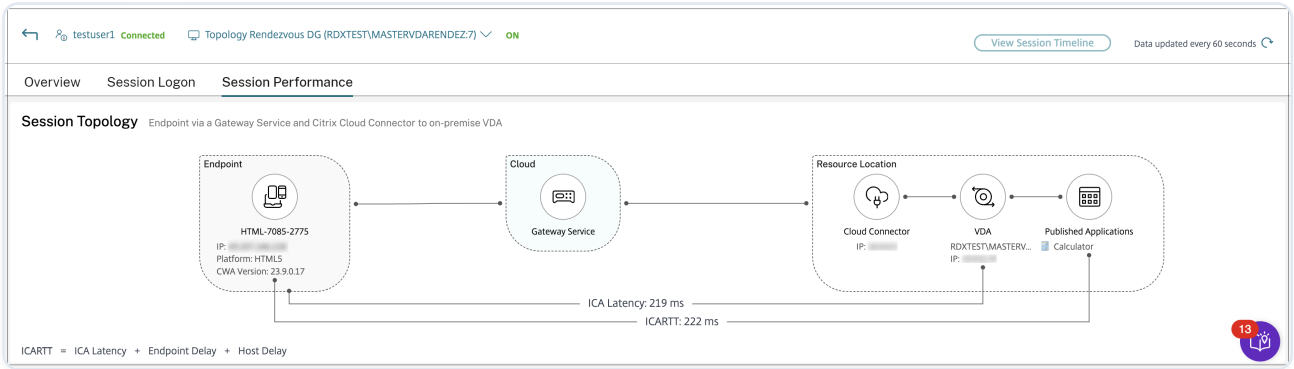
- Aplicativo Citrix Workspace no Endpoint
- Serviço Gateway/Gateway local
- Cloud Connector – O Gateway está conectado ao DaaS por meio de um Cloud Connector no caso de conexões híbridas.
- VDAs

Consequentemente, as possíveis topologias de rede são as seguintes:

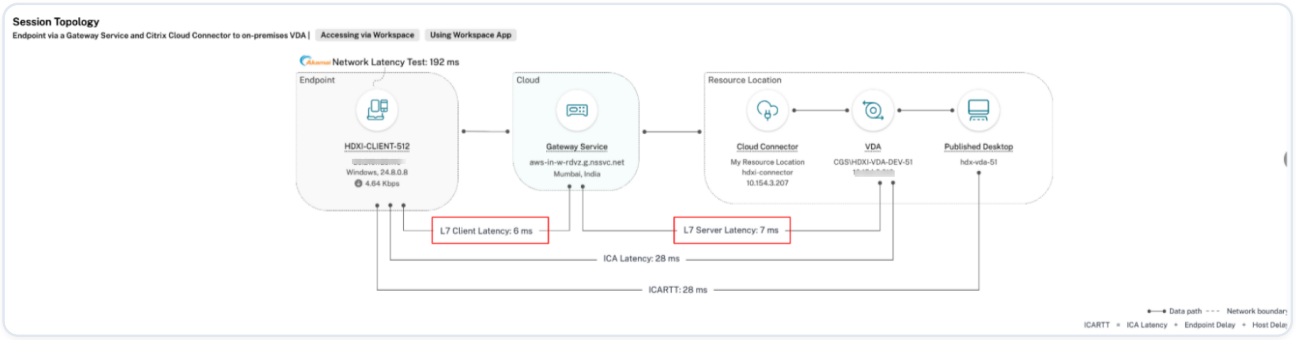
- O aplicativo Citrix Workspace no endpoint se conecta via Citrix® StoreFront Cloud e Gateway Service a um VDA local. Nenhum Cloud Connector é usado para se conectar ao VDA.



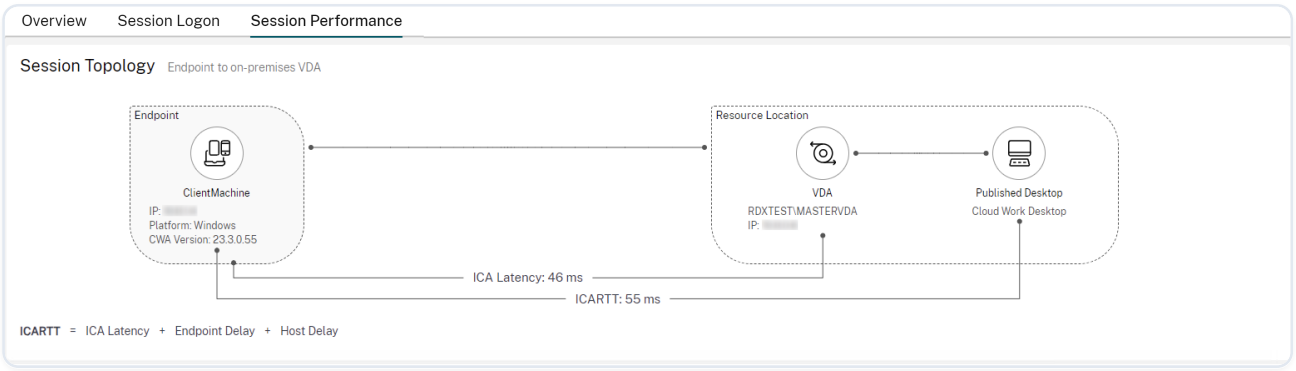
- O aplicativo Citrix Workspace no endpoint se conecta via Citrix® StoreFront Cloud e Gateway Service a um VDA local via Cloud Connector.



- O aplicativo Citrix Workspace no endpoint se conecta via StoreFront™ e Gateway local a um VDA local.



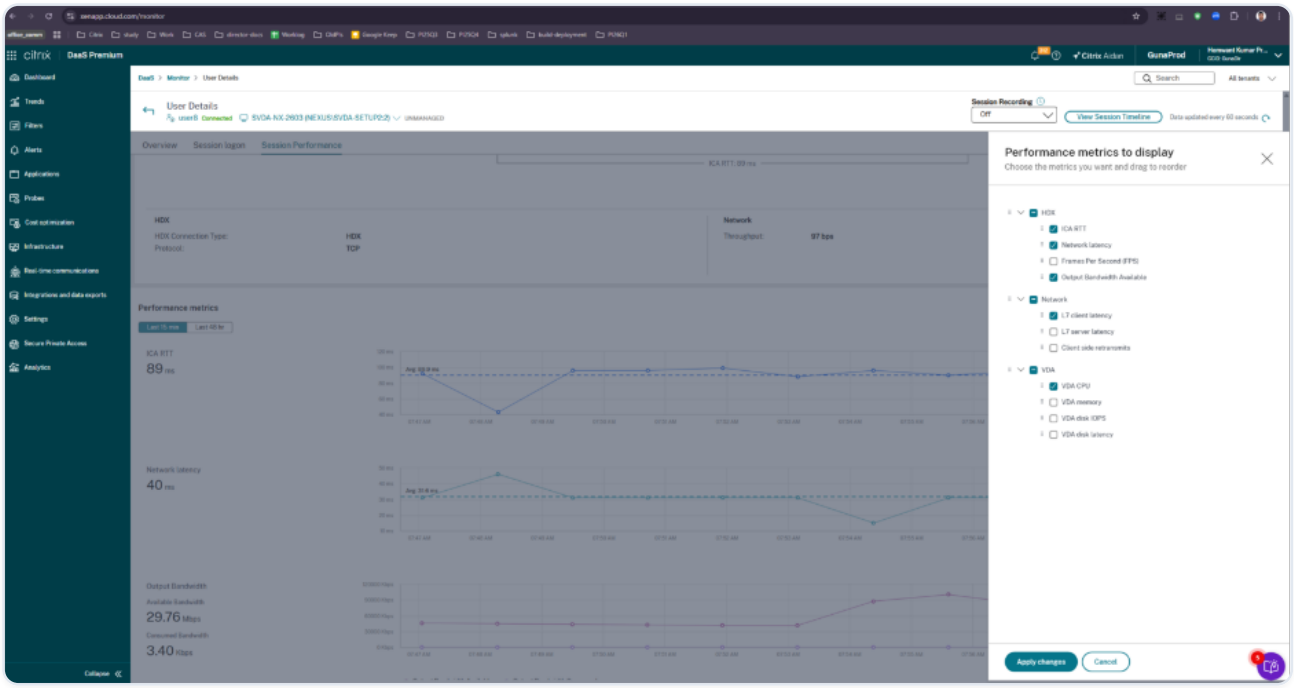
- O aplicativo Citrix Workspace no endpoint se conecta via StoreFront a um VDA local.



Métricas de Desempenho

O painel **Métricas de Desempenho** oferece a capacidade de correlacionar métricas em tempo real na identificação de problemas dentro das sessões do usuário. As tendências para as métricas de sessão ajudam a indicar como essas métricas se comportaram ao longo do tempo. Ao clicar na guia **Desempenho da Sessão**, juntamente com os dados em tempo real, você pode visualizar os dados dos últimos 15 minutos e 48 horas. Os gráficos ajudam a correlacionar múltiplas métricas de desempenho de componentes em uma única visualização.

Use a opção *Gerenciar* nesta seção para escolher as métricas relevantes que você deseja visualizar e correlacionar para o usuário em questão.



Nota:

- Com o suporte a métricas dos últimos 15 minutos, o gráfico é plotado para a duração em que a sessão está conectada e desconectada. A métrica da sessão desconectada é exibida com o valor zero.
- Com o suporte a métricas das últimas 48 horas, os gráficos de ICARTT, Latência ICA e Reconexões de Sessão são atualizados com as métricas de dados históricos. As informações de reconexão de sessão ajudam você a visualizar e solucionar problemas de conexões de rede com interrupções. Também analisa redes com uma experiência contínua. O gráfico para ver o número de Reconexões de Sessão, Reconexões Totais de Sessão, Reconexão automática do cliente e Reconexões de confiabilidade da sessão.

Além de ICARTT e Latência ICA, as seguintes métricas estão disponíveis para métricas em tempo real e dos últimos 15 minutos:

- Quadros por Segundo - Quadros por Segundo é uma métrica importante que indica a capacidade de resposta da sessão.
- Largura de Banda de Saída Disponível - Largura de Banda de Saída Disponível é uma medida da largura de banda total disponível para transmitir dados do VDA para o endpoint.

- Largura de Banda de Saída Consumida - Largura de Banda de Saída Consumida indica a quantidade real de dados transmitidos do VDA para o endpoint para exibir sessões aos usuários.

Analisar a Largura de Banda de Saída Disponível e a Largura de Banda de Saída Consumida ajuda a verificar se há largura de banda suficiente para atender às sessões e a detectar se uma sessão é afetada por largura de banda insuficiente.

Solucionar problemas quando os dados de ICA RTT ou Duração de Logon da Sessão não são preenchidos

Anteriormente, quando o serviço EUEM ou o serviço Profile Management falhava ao ser executado, o motivo da falha na obtenção dos dados relacionados ao ICA RTT ou Duração de Logon da Sessão não era exibido. Com este novo recurso, você pode obter o motivo da falha e a solução correspondente para essa falha. Os links **Saiba mais** fornecem os erros de ICA RTT e Duração de Logon da Sessão, o motivo da falha e a solução, conforme mencionado na tabela a seguir:

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
Erro de ICA RTT	O valor de ICA RTT não é exibido.	**O Citrix End User Experience Monitoring não está em execução.**	`1.` Abra o console de Serviços. Para abrir este console, clique em **Iniciar** e digite **Serviços**.
			`2.` Certifique-se de que o Serviço de Monitoramento da Experiência do Usuário Final do Citrix esteja em execução.
			`3.` Reabra a sessão da área de trabalho e tente novamente. O valor de ICA RTT deve ser exibido.

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
			4. Se o problema persistir, entre em contato com o administrador do Citrix.
Erro de ICA RTT	O valor de ICA RTT não é exibido.	**O Monitoramento da Experiência do Usuário Final do Citrix não está instalado.**	1. Reinstale o VDA.
			2. Abra o console de Serviços. Para abrir este console, clique em **Iniciar** e digite Serviços
			3. Certifique-se de que o Serviço de Monitoramento da Experiência do Usuário Final do Citrix esteja em execução.
			4. Reabra a sessão da área de trabalho e tente novamente. O valor de ICA RTT deve ser exibido agora.
			5. Se o problema persistir, entre em contato com o administrador do Citrix.
Erro de ICA RTT	O valor de ICA RTT não é exibido.	**Erro ao buscar dados.**	1. Abra o console de Serviços. Para abrir este console,

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
			clique em **Iniciar** e digite Serviços.
			`2.` Certifique-se de que o **Serviço de Instrumentação de Gerenciamento do Windows** esteja em execução.
			`3.` Além disso, certifique-se de que o processo WfShell.exe/ PicaShell.exe esteja em execução em **Gerenciador de Atividades** > guia **Processo**. Se não estiver em execução, reabra a sessão da área de trabalho.
			`4.` Se as etapas anteriores não estiverem funcionando, execute o seguinte comando para garantir que a instância Citrix_Euem_Round Trip esteja presente: `Get-CimInstance -Namespace 'ROOT\Citrix\Euem' -Query "select * from Citrix_Euem_Round Trip"`

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
			5. Se a instância Citrix_Euem_Round Trip estiver presente, reabra a sessão da área de trabalho.
			6. Se o problema persistir, entre em contato com o administrador Citrix.
Erro de Duração de Logon da Sessão	O gráfico não foi carregado.	**O Citrix Profile Management não está em execução**	1. Abra o console de Serviços. Para abrir este console, clique em **Iniciar** e digite Serviços.
			2. Certifique-se de que o **Serviço de Gerenciamento de Perfil Citrix** esteja em execução.
			3. Reabra a sessão da área de trabalho e tente novamente. O gráfico deve ser exibido.
			4. Se o problema persistir, entre em contato com o administrador Citrix.
Erro de Duração de Logon da Sessão	O gráfico não foi carregado.	**O Citrix Profile Management não está instalado.**	1. Instale o Serviço de Gerenciamento de Perfil Citrix.

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
			2. Abra o console de Serviços. Para abrir este console, clique em **Iniciar** e digite Serviços.
			3. Certifique-se de que o **Citrix Profile Management Service** esteja em execução.
			4. Reabra a sessão da área de trabalho e tente. O gráfico deve ser exibido.
			5. Se o problema persistir, entre em contato com o administrador do Citrix.
Erro de Duração de Logon da Sessão	O gráfico não é carregado.	**Erro ao buscar dados.**	1. Abra o console de **Serviços**. Para abrir este console, clique em **Iniciar** e digite Serviços.
			2. Certifique-se de que o **Serviço de Instrumentação de Gerenciamento do Windows** esteja em execução.
			3. Se o serviço anterior já estiver em execução, execute o

TIPO DE ERRO	ERRO	MENSAGEM DE ERRO	SOLUÇÃO
			seguinte comando para garantir que `LogonTimings instance is present`: `Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics' -Query "select * from LogonTimings"`
			`4.` Se o problema persistir, entre em contato com o administrador Citrix.
Erro de ICA RTT	O valor de ICA RTT não é exibido.	O console não é compatível.	Inicie uma sessão usando HDX.
Erro de ICA RTT	O valor de ICA RTT não é exibido.	O Protocolo de Área de Trabalho Remota (RDP) não é compatível.	Inicie uma sessão usando HDX.
Erro de ICA RTT	O valor de ICA RTT não é exibido.	Atualize o VDA para a versão 2402 ou superior para obter detecção detalhada de erros e acessar todos os recursos.	Atualize o VDA para 2402 ou superior.
Erro de Duração de Logon da Sessão	O gráfico não é carregado.	O plug-in WMI do Citrix Profile Management não está instalado.	Instale o plug-in WMI do Citrix Profile Management.

Diagnosticar problemas de desempenho de aplicativos

O monitoramento de desempenho de aplicativos no Citrix Director (integrado ao uberAgent) fornece aos administradores insights granulares sobre como os aplicativos individuais — tanto publicados quanto locais — estão se comportando. Esses dados ajudam a identificar se um problema é causado pelo consumo de recursos do aplicativo, dependências de rede ou falta de resposta da interface do usuário.

Pré-requisitos

- A versão do VDA Windows deve ser maior ou igual a 2603
- O uberAgent deve ser instalado nos VDAs
- A política "Aprimorar o Director com dados do uberAgent para desempenho de aplicativos" deve ser habilitada no Studio.

NOME DA POLÍTICA	DESCRIÇÃO DA POLÍTICA	MÉTRICAS DA UI	VALOR PADRÃO	OPÇÕES DE VALOR	VERSÃO DO VDA WINDOWS	VDA (LINUX, MAC)
Aprimorar o Director com dados do uberAgent para desempenho de aplicativos	Permite que o Director use dados de métricas da máquina fornecidos pelo uberAgent para desempenho de aplicativos	Nome do aplicativo, Está publicado, Nome do processo, Uso da CPU %, Uso da memória %, Memória do conjunto de trabalho (MB), IOPS do disco, Latência do disco (ms),	Ativado	Ativado ou Desativado	2603 ou posterior	Não Disponível

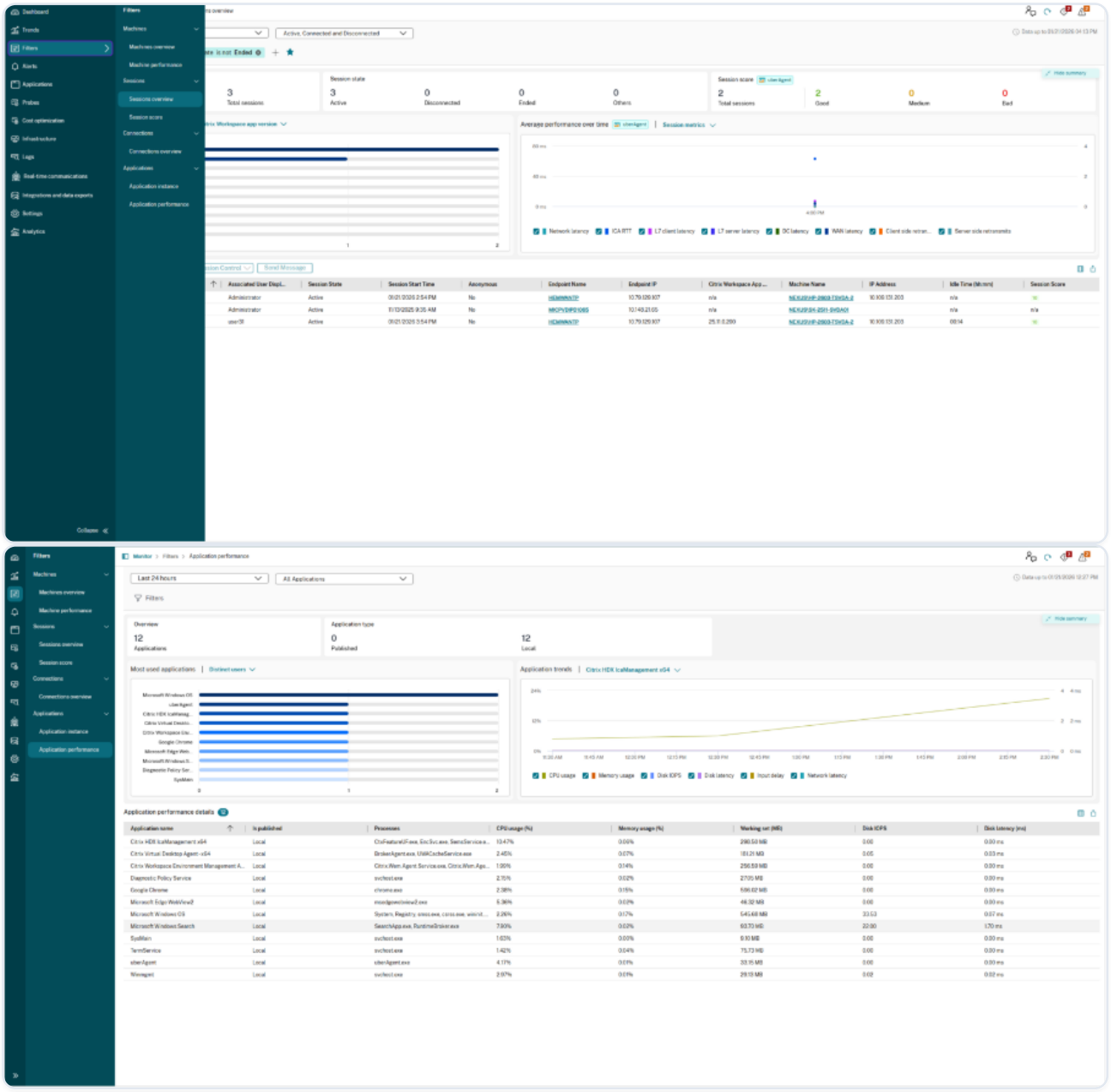
NOME DA POLÍTICA	DESCRIÇÃO DA POLÍTICA	MÉTRICAS DA UI	VALOR PADRÃO	OPÇÕES DE VALOR	VERSÃO DO VDA WINDOWS	VDA (LINUX, MAC)
		Latência da rede (ms), Atraso de entrada (ms), Uso da CPU % (P95), Uso da memória % (P95), Atraso de entrada (P95) (ms), Falha de página por segundo				

Visão Geral e Principais Recursos

Esta página detalha a documentação para a nova guia **Desempenho do Aplicativo**, que se concentra no monitoramento em tempo real e histórico de aplicativos publicados e locais.

Os principais recursos são:

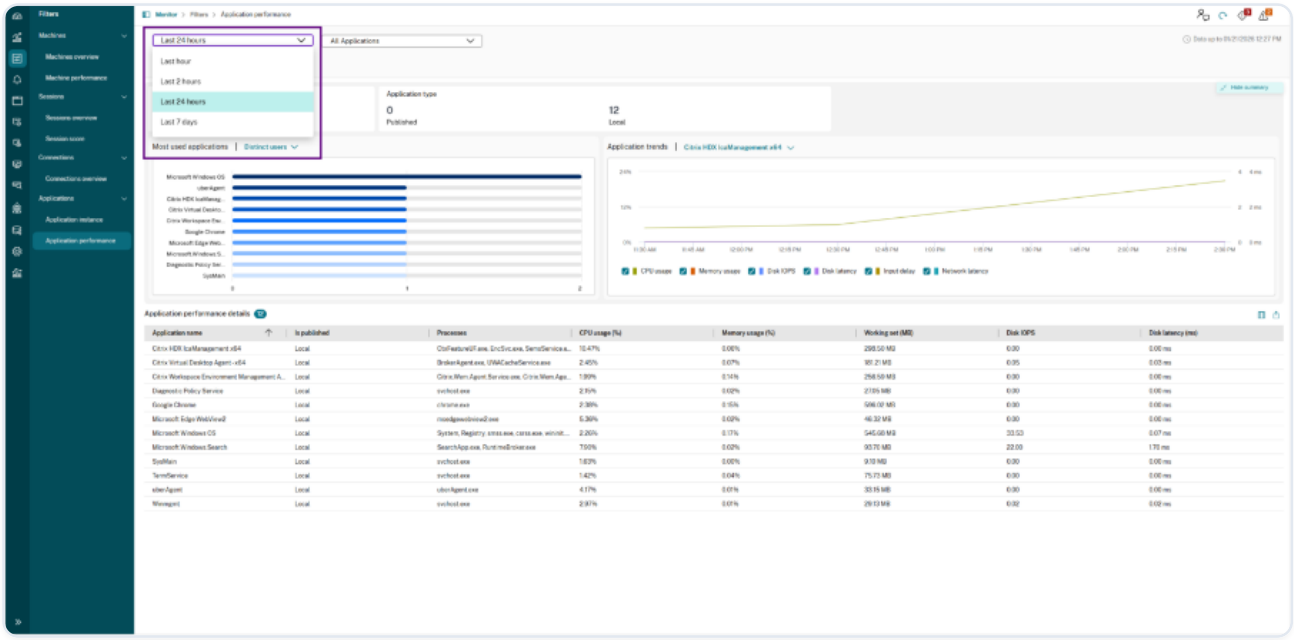
- Filtros de Intervalo de Tempo: Precisão de monitoramento aprimorada com opções de intervalo de tempo.
- Gerenciamento Simplificado de Filtros: Menu suspenso intuitivo para gerenciar filtros.
- Criação Intuitiva de Filtros: Fluxo de trabalho flexível para criar e modificar filtros diretamente na página principal.
- Visualizações: Introdução do gráfico de Distribuição de Aplicativos e do gráfico de Desempenho ao Longo do Tempo para uma visão imediata das tendências de desempenho de aplicativos.



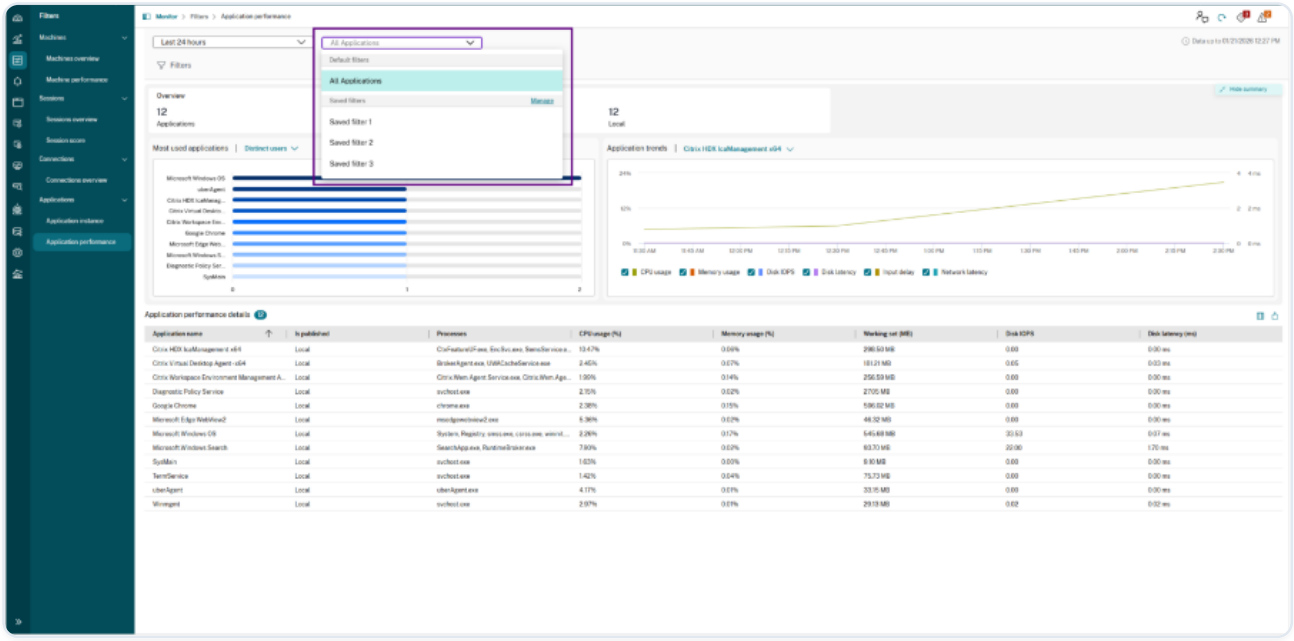
Filtrando Dados

Na parte superior da página, você pode definir o escopo dos dados exibidos.

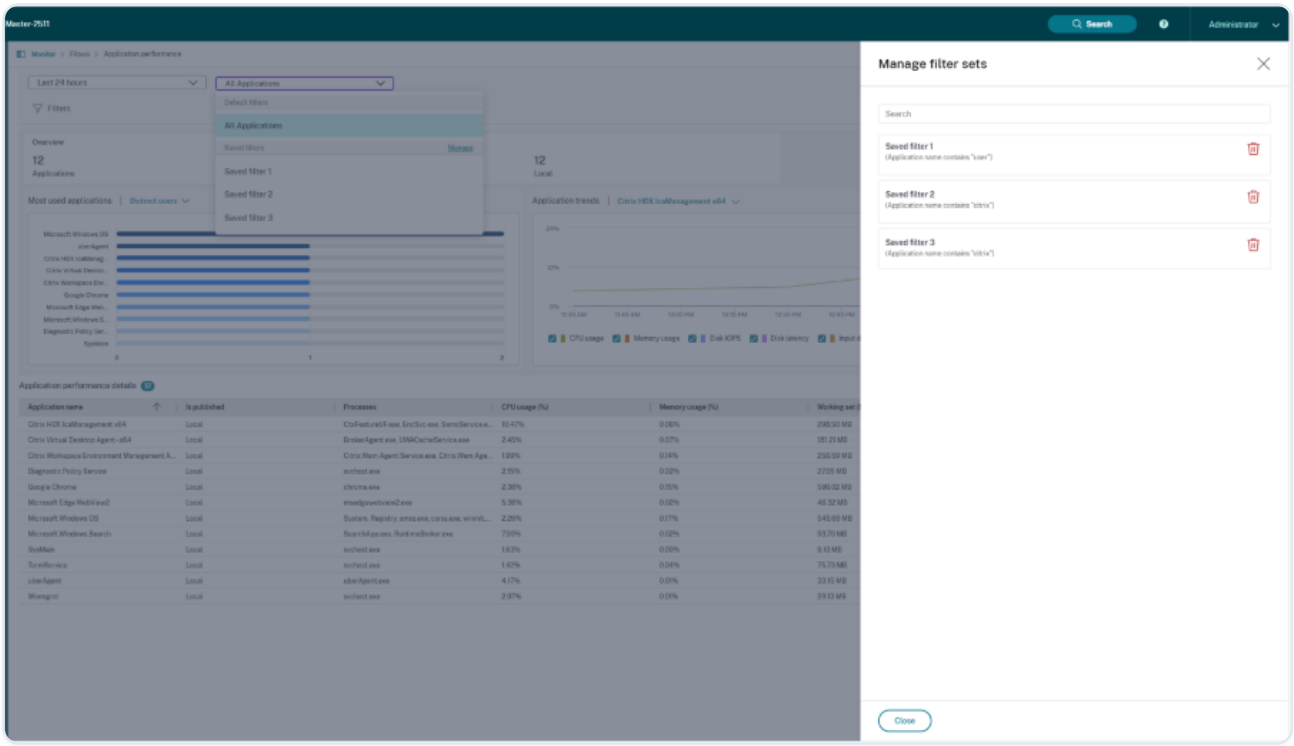
- **Período:** Escolha o intervalo de tempo. O filtro de intervalo de tempo inclui 1 hora, 2 horas, 1 dia ou sete dias



- **Escopo do Aplicativo:** Use o menu suspenso do aplicativo para filtrar todo o painel por um filtro específico ou visualizar **Todos os Aplicativos**.



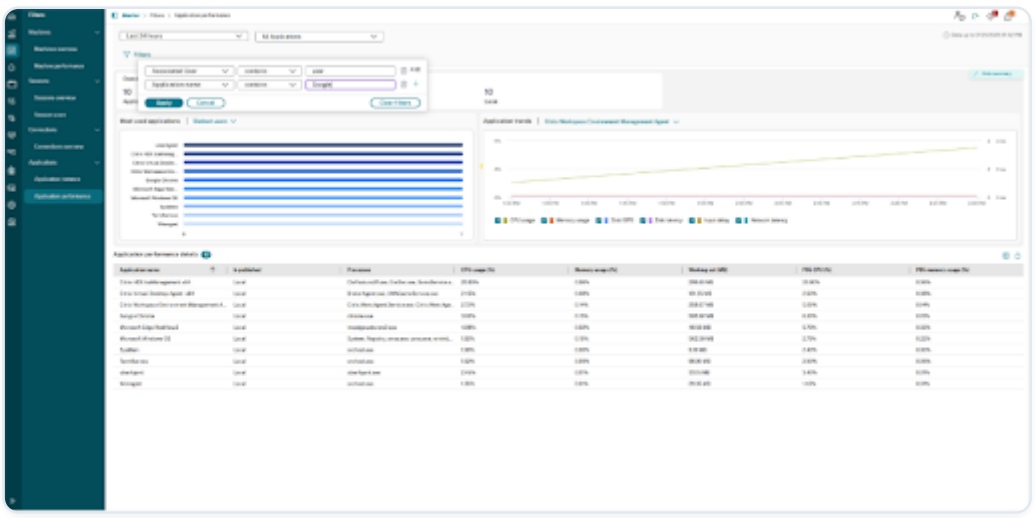
- **Filtros:** Use o ícone Filtros para refinar ainda mais os dados.
- **Gerenciar:** Clicar em Gerenciar abre um painel lateral onde você pode pesquisar, visualizar ou excluir filtros salvos existentes.

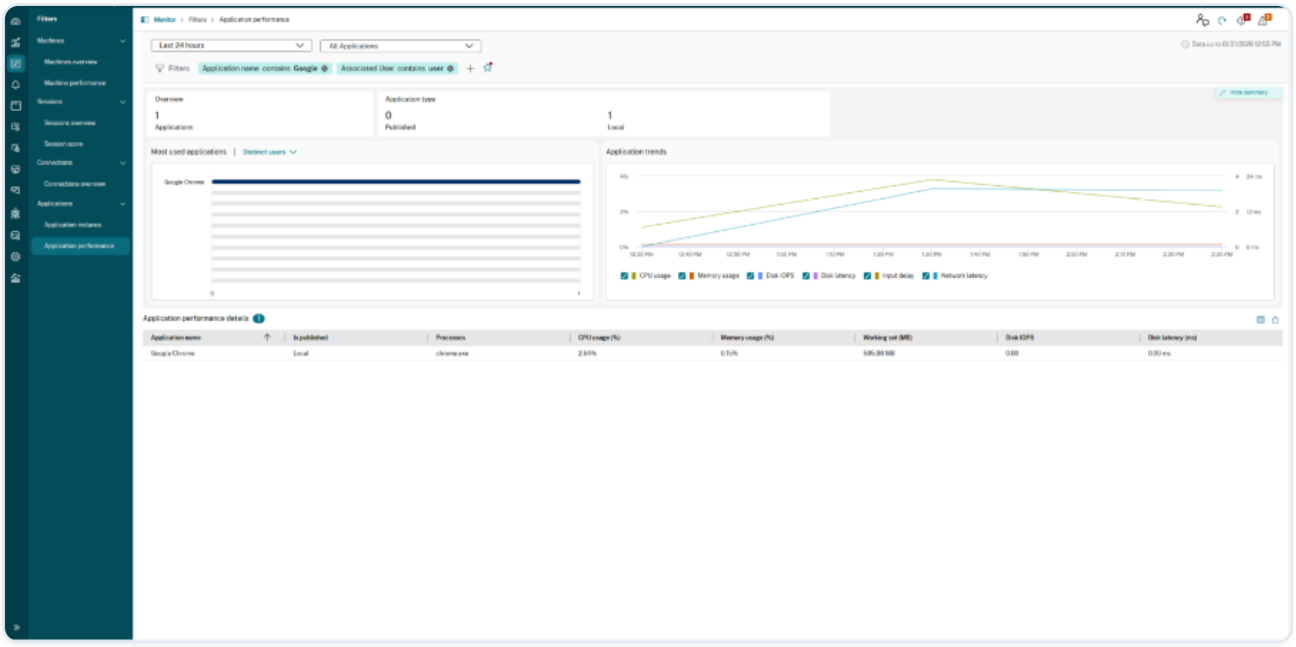


Criando e Aplicando Filtros

Agora você pode criar conjuntos de filtros complexos diretamente na página de visão geral dos aplicativos:

- Clique no ícone Filtros ou no botão + ao lado de um filtro existente.
- Selecione os critérios (por exemplo, Nome do aplicativo), o operador (por exemplo, contém) e o valor (por exemplo, Google).





STATUS DE SALVAMENTO E FLUXO DE TRABALHO DO FILTRO

O ícone de estrela (⋆) ao lado dos filtros ativos indica visualmente o status do seu conjunto de filtros atual. Isso ajuda a guiar os administradores para salvar, aplicar e gerenciar filtros personalizados.

STATUS DO FILTRO	APARÊNCIA DO ÍCONE	SIGNIFICADO	AÇÃO NECESSÁRIA
Filtro Não Salvo	 (Contorno vazio com um Ponto Vermelho)	A combinação atual de critérios de filtro **não foi salva**.	Clique na **estrela vazia** para abrir a caixa de diálogo, nomear o conjunto de filtros e salvá-lo.
Filtro Salvo	 (Preenchido / Sólido)	O conjunto de filtros atualmente ativo é uma **correspondência exata** com um filtro salvo anteriormente.	Nenhuma ação necessária. Você está visualizando dados com base em um modelo definido.
Filtro Salvo com Alterações		Ao usar um **filtro salvo**, se qualquer outro filtro for adicionado, removido ou se qualquer coluna for	Clique na **estrela com ponto vermelho** para atualizar o filtro salvo existente, ou use o menu suspenso para

STATUS DO FILTRO	APARÊNCIA DO ÍCONE	SIGNIFICADO	AÇÃO NECESSÁRIA
	(Preenchido com Ponto Vermelho)	classificada, o ponto vermelho aparecerá, o que significa que as alterações **ainda não foram salvas**.	selecionar **Salvar como conjunto de filtros** para criar um novo.

BOTÕES DE AÇÃO DO FILTRO

Ao adicionar novos filtros ou modificar um filtro salvo, os seguintes controles e indicadores de status ficam disponíveis:

BOTÃO	SIGNIFICADO E AÇÃO
Atualizar	Aplica todos os critérios de filtro atualmente ativos aos gráficos e à tabela de dados de desempenho do aplicativo.
Cancelar	Descarta quaisquer alterações feitas no conjunto de filtros atual e reverte para o último filtro aplicado.
Limpar filtros	Remove todos os critérios de filtro recém-adicionados.
 **Ícone**	Remove os critérios de filtro selecionados nos quais este ícone é clicado.

Visualização

RESUMO DA VISÃO GERAL

O painel de resumo fornece uma contagem imediata dos aplicativos atualmente monitorados:

- **Aplicativos:** O número total de nomes de aplicativos exclusivos detectados no ambiente.
- **Tipo de Aplicativo:** Uma análise de quantas são aplicações **Publicadas** versus aplicações **Locais** sendo executadas no VDA.

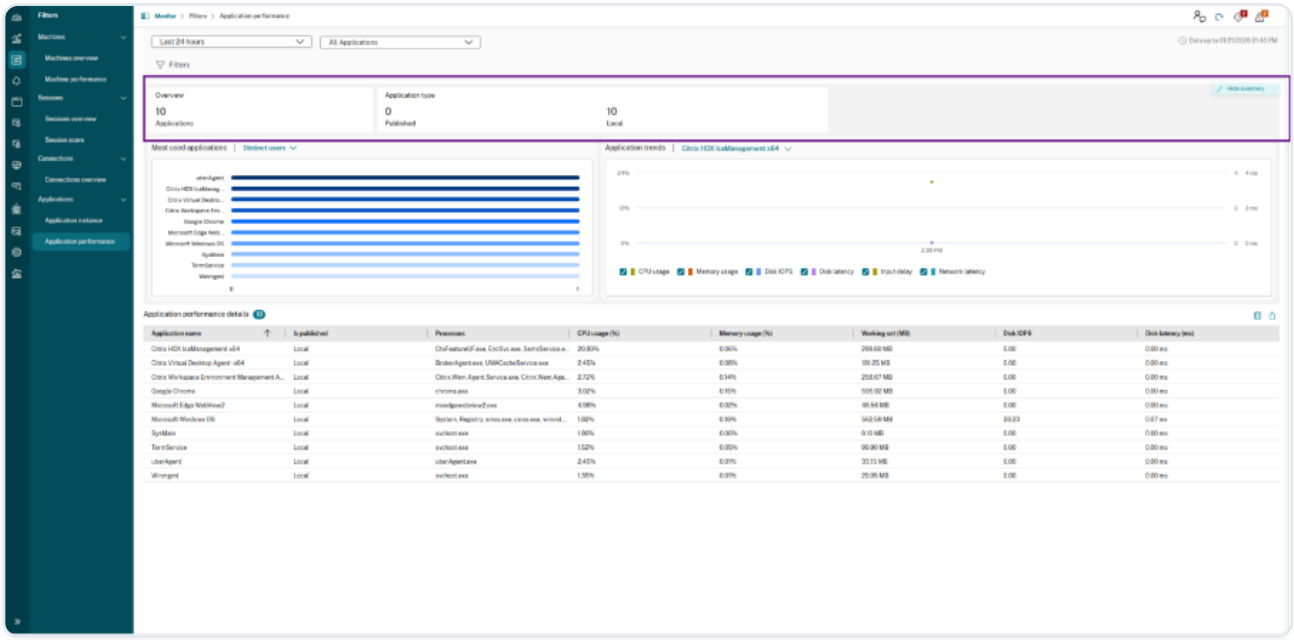


Gráfico de Distribuição

O gráfico de Distribuição serve como um histograma que categoriza o número de instâncias de aplicativos com base em buckets de desempenho específicos. Ele foi projetado para ajudá-lo a entender a "distribuição" da experiência do usuário em seu ambiente.

- **Agrupamento de Métricas:** O eixo X representa intervalos da métrica selecionada (como **Atraso da UI** ou **Duração da Inicialização**), enquanto o eixo Y representa a contagem de ocorrências dentro desses intervalos.
- **Perspectivas de Visualização:** Um menu suspenso permite alternar a representação dos dados entre duas visualizações:
  - **Usuários Distintos:** Mostra a distribuição do desempenho com base no número de usuários únicos
  - **Máquinas Distintas:** Mostra a distribuição com base no número de VDAs.

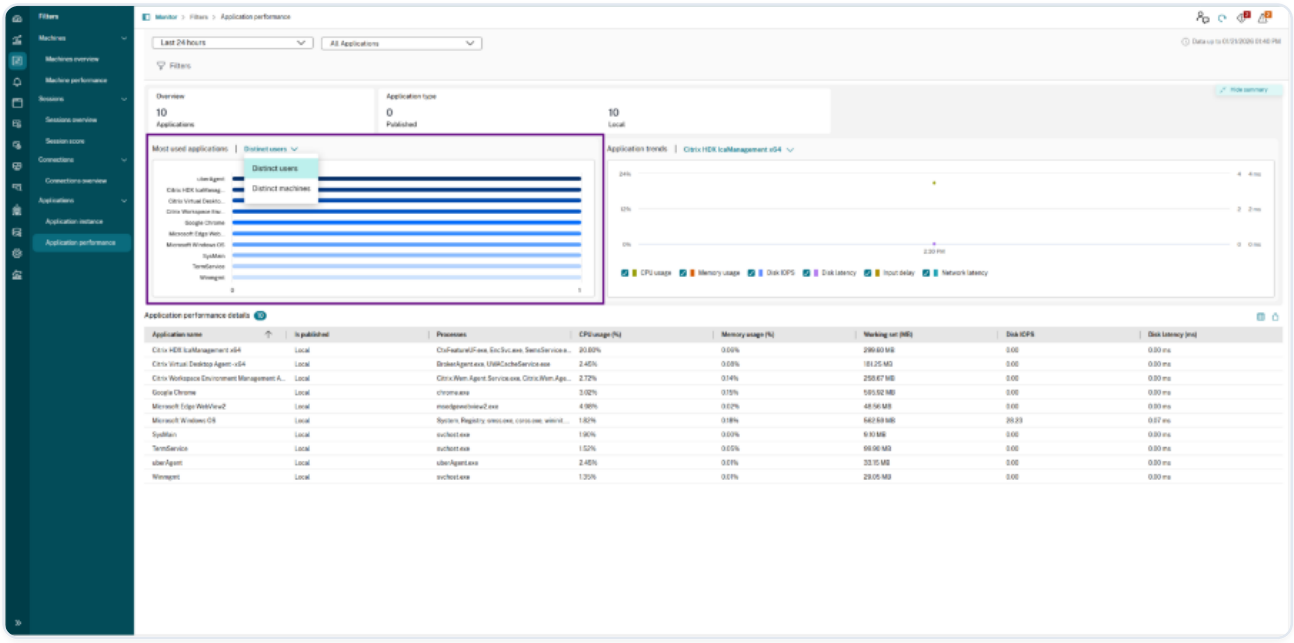
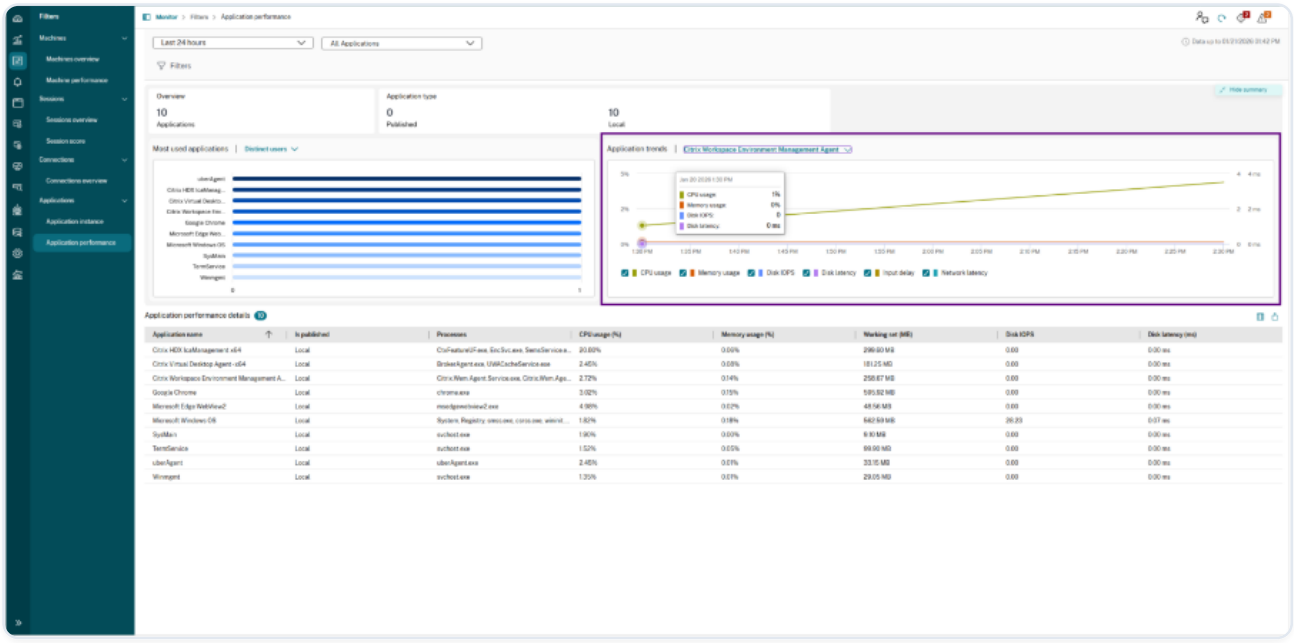


Gráfico de Desempenho

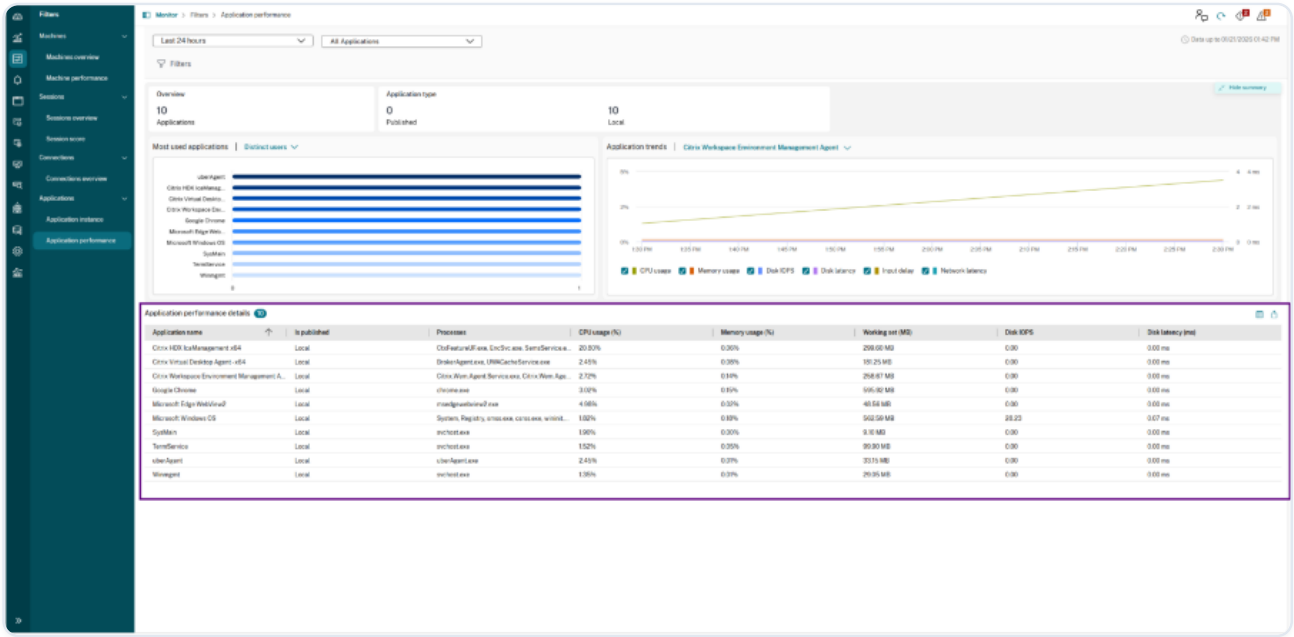
O gráfico de Desempenho é uma visualização de série temporal que rastreia a integridade do aplicativo durante uma duração selecionada. Ele permite correlacionar mudanças de desempenho com intervalos de tempo específicos e consumo de recursos.

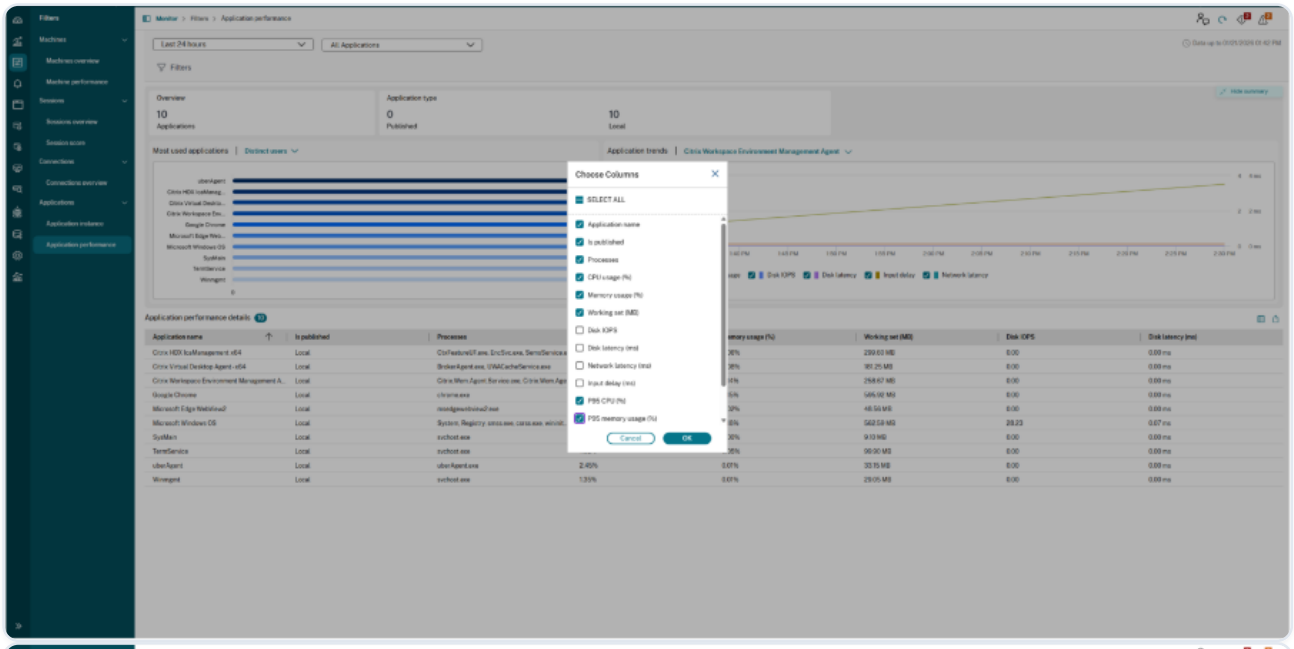
- **Seleção de Aplicativo:** Use o menu suspenso na parte superior do gráfico para selecionar um aplicativo específico para analisar.
- **Correlação Multimétrica**: O gráfico permite sobrepor vários indicadores-chave de desempenho (KPIs) simultaneamente para encontrar correlações entre capacidade de resposta e uso de recursos:
  - **Uso de CPU e Memória**: Exibe a porcentagem de consumo de recursos pelo aplicativo.
  - **IOPS de Disco e Latência de Disco**: Identifica se gargalos de armazenamento estão impactando o desempenho do aplicativo.
  - **Atraso de Entrada**: Mede o tempo entre uma ação do usuário e a resposta do aplicativo.
  - **Latência de Rede**: Rastreia o atraso da rede associado à comunicação do aplicativo.

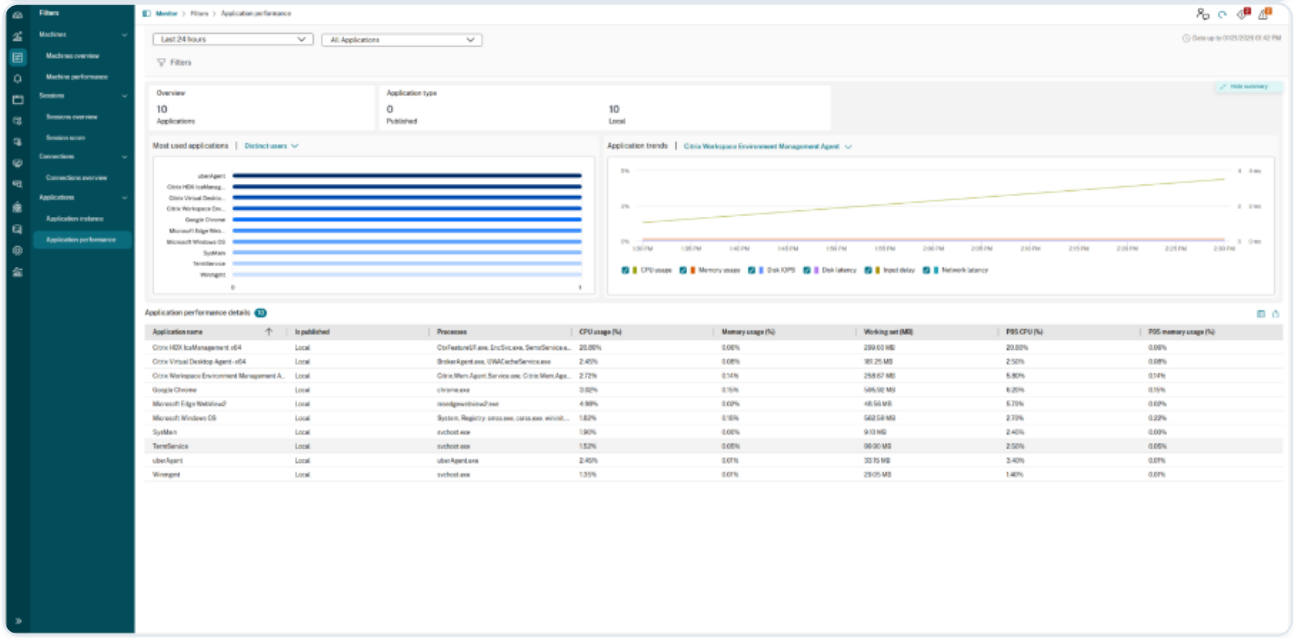


Detalhes de Desempenho do Aplicativo (Tabela)

O painel inferior fornece os dados brutos e acionáveis para cada instância do aplicativo. Os dados podem ser exportados, e as colunas desejadas podem ser escolhidas para exibição.







Diagnosticar sessões de usuário históricas

O Citrix Monitor agora exibe os detalhes das sessões em estado ativo, desconectado ou encerrado. Anteriormente, você só podia ver os detalhes das sessões ativas. Com este recurso, os administradores de help desk podem solucionar problemas com uma sessão que foi encerrada ou está em estado encerrado. Os detalhes das sessões encerradas estão disponíveis para as últimas 24 horas e os últimos 2 dias. Você pode visualizar os seguintes detalhes de uma sessão encerrada ou terminada:

- Painel Detalhes da Máquina - Exibe os detalhes disponíveis da máquina onde a sessão selecionada foi iniciada
- Painel Detalhes da Sessão - Exibe os detalhes disponíveis da sessão selecionada.

- Duração do logon da sessão - Exibe as informações sobre a duração do logon para a sessão selecionada. Você pode visualizar o gráfico sobre o tempo gasto para o seguinte:
  - Intermediação
  - Inicialização da máquina
  - Conexão HDX™
  - Autenticação
  - GPOs
  - Scripts de logon
  - Carregamento de perfil em disco
  - Sessão interativa

Para visualizar as sessões de usuário históricas, faça o seguinte:

1. Clique em **Filtrar** > visualização **Sessão**.
2. Clique em **Usuário Associado** para abrir o Gerenciador de Atividades para o usuário.

   Gerenciador de Atividades de sessões de usuário históricas(/en-us/citrix-daas/media/dir-his-user-sessions-am.png)
3. Selecione a sessão necessária na seção **Sessões Encerradas**.
4. Visualize os painéis **Detalhes da Máquina** e **Detalhes da Sessão**.

   Detalhes das sessões de usuário históricas(/en-us/citrix-daas/media/dir-his-user-sessions-details.png)
5. Role para baixo e visualize a **duração do logon da sessão** para a sessão encerrada.

   Duração das sessões de usuário históricas(/en-us/citrix-daas/media/dir-his-user-sessions-duration.png)
6. Clique na guia **Logon da Sessão** e visualize os detalhes.

   Duração do logon de sessões de usuário encerradas(/en-us/citrix-daas/media/session-logon-ended.png)
7. Clique na guia **Desempenho da Sessão** e visualize os detalhes.

   Desempenho de sessões de usuário encerradas(/en-us/citrix-daas/media/session-performance-ended.png)

Usuários sombra

Use o recurso de usuário sombra para visualizar ou trabalhar diretamente na máquina virtual ou sessão de um usuário. Você pode sombrear VDAs Windows e Linux. O usuário deve estar conectado à máquina que você deseja sombrear. Verifique isso consultando o nome da máquina listado na barra de título do usuário.

O sombreamento é iniciado em uma nova guia; atualize as configurações do seu navegador para permitir pop-ups do URL do Citrix Cloud™.

Acesse o recurso de sombreamento na exibição **Detalhes do Usuário**. Selecione a sessão do usuário e clique em **Sombrear** na exibição Gerenciador de Atividades ou no painel Detalhes da Sessão.

Sombreamento de VDAs Linux

O sombreamento está disponível para VDAs Linux Versão 7.16 ou posterior executando as distribuições Linux RHEL7.3 ou Ubuntu Versão 16.04.

> **Nota:**
>
> - O Monitor usa FQDN para se conectar ao VDA Linux de destino. Certifique-se de que o cliente Monitor possa resolver o FQDN do VDA Linux.
> - O VDA deve ter os pacotes python-websockify e x11vnc instalados.
> - A conexão noVNC com o VDA usa o protocolo WebSocket. Por padrão, o protocolo WebSocket **ws://** é usado. Por motivos de segurança, a Citrix recomenda que você use o protocolo seguro **wss://**. Instale certificados SSL em cada cliente Monitor e VDA Linux.

> Siga as instruções em Sombreamento de Sessão para configurar seu VDA para sombreamento.

1. Depois de clicar em **Sombrear**, a conexão de sombreamento é inicializada e um prompt de confirmação aparece no dispositivo do usuário.
2. Instrua o usuário a clicar em **Sim** para iniciar o compartilhamento da máquina ou da sessão.
3. O administrador pode apenas visualizar a sessão sombreada.

Sombreamento de VDAs Windows

As sessões VDA do Windows são espelhadas usando o Assistência Remota do Windows. Habilite o recurso Assistência Remota do Windows do Usuário durante a instalação do VDA. Para obter mais informações, consulte Habilitar ou Desabilitar recursos.

1. Depois de clicar em **Espelhar**, a conexão de espelhamento é inicializada e uma caixa de diálogo solicita que você abra ou salve o arquivo de incidente .msrc.
2. Abra o arquivo de incidente com o Visualizador de Assistência Remota, se ainda não estiver selecionado por padrão. Um prompt de confirmação aparece no dispositivo do usuário.
3. Instrua o usuário a clicar em **Sim** para iniciar o compartilhamento da máquina ou da sessão.
4. Para mais controle, peça ao usuário para compartilhar o controle do teclado e do mouse.

OTIMIZAR NAVEGADORES MICROSOFT INTERNET EXPLORER PARA ESPELHAMENTO

Configure seu navegador Microsoft Internet Explorer para abrir automaticamente o arquivo Microsoft Remote Assistance (.msra) baixado com o cliente de Assistência Remota.

Para fazer isso, você deve habilitar a configuração Solicitação automática para downloads de arquivos no editor de Política de Grupo:

Configuração do Computador \> Modelos Administrativos \> Componentes do Windows \> Internet Explorer \> Painel de Controle da Internet \> Página de Segurança \> Zona da Internet \> Solicitação automática para downloads de arquivos.

Usando o Compartilhamento de Tela HDX

O Director oferece suporte à assistência remota que permite que administradores de TI e pessoal de suporte técnico forneçam suporte remoto a usuários finais por meio da tecnologia de compartilhamento de tela HDX. Esse recurso aproveita o protocolo HDX nativo da Citrix para oferecer recursos de compartilhamento de tela seguros e de alto desempenho para cenários de solução de problemas e assistência ao usuário.

PRÉ-REQUISITOS

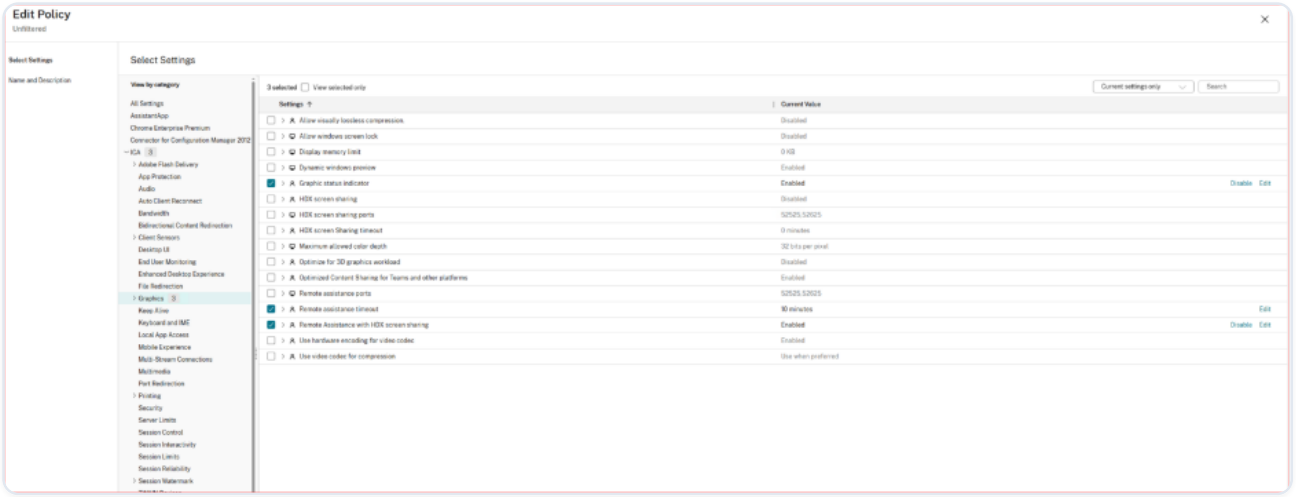
COMPONENTE	AMBIENTES OU VERSÕES SUPORTADOS
Sistemas Operacionais	Windows, Linux para SO de Sessão Única **ou SO de Múltiplas Sessões**
Virtual Delivery Agent (VDA)	CR 2511 ou superior
Director	CR 2511 ou superior

COMPONENTE	AMBIENTES OU VERSÕES SUPORTADOS
Delivery Controller	CR 2511 ou superior
TWPlayer (ThinWire Player)	Um link para baixar o player está disponível na interface do usuário do Director ao iniciar uma sessão de sombra

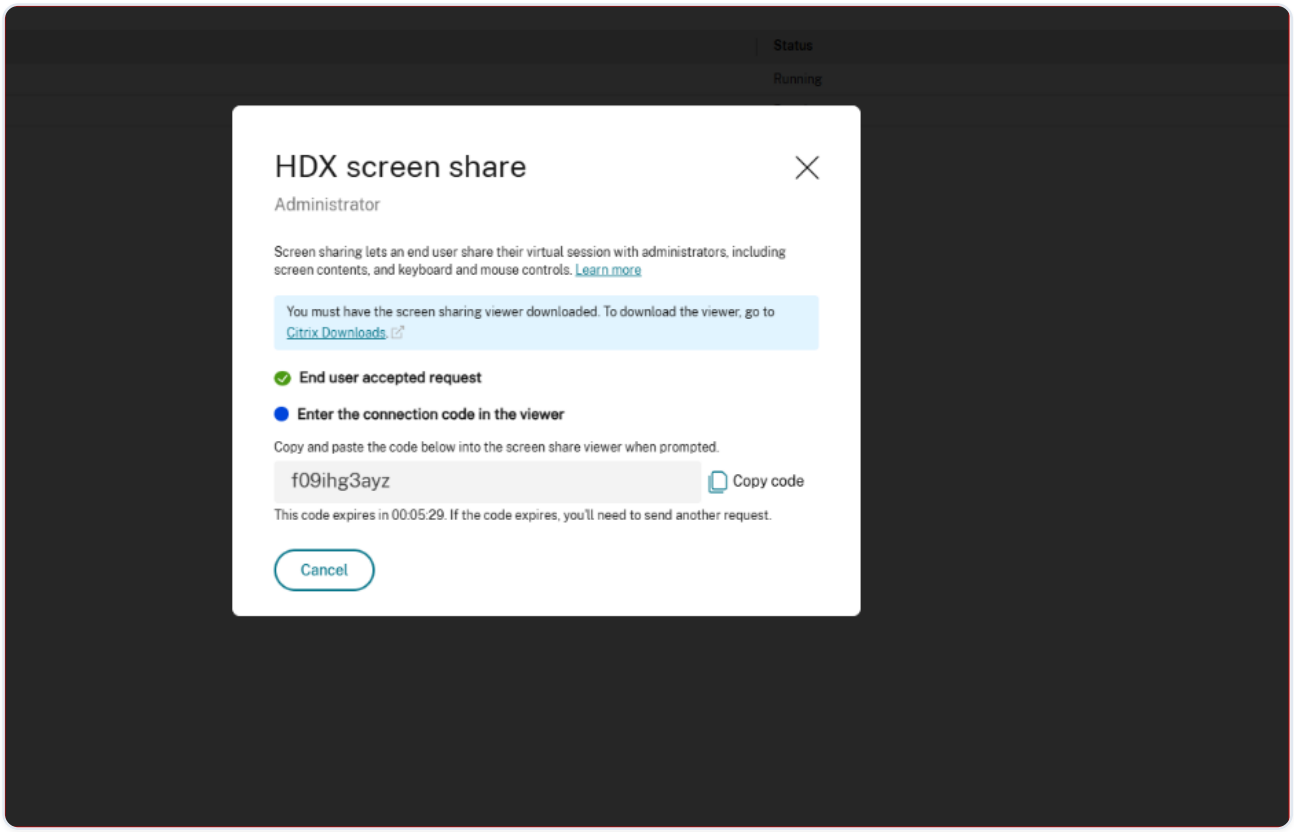
CONFIGURAÇÃO DE POLÍTICA DE GRUPO

Para habilitar a Assistência Remota usando o Director e o HDX Screen Share, configure as seguintes Políticas de Grupo no VDA:

- Assistência Remota com compartilhamento de tela HDX
- Tempo limite da assistência remota
- Indicador de Status Gráfico



TWPlayer (ThinWire Player) é um componente obrigatório que deve ser baixado uma vez para habilitar a funcionalidade de compartilhamento de tela HDX. Um link para baixar o player está disponível na interface do usuário do Director ao iniciar uma sessão de sombra.



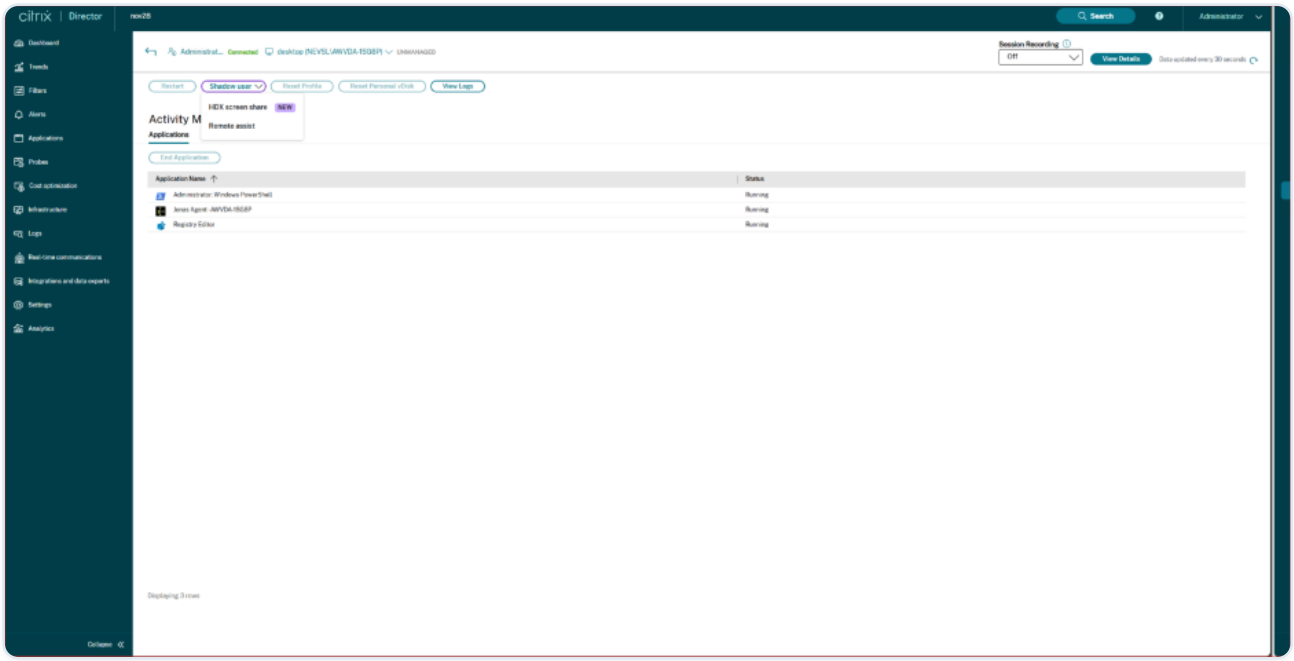
Limitações

- Aplicativos publicados (sessões de aplicativo) não podem ser sombreados – apenas sessões de desktop.

Fluxo de trabalho usando o Director e o Compartilhamento de Tela HDX
As etapas abaixo descrevem o processo para um administrador iniciar uma sessão de compartilhamento de tela HDX:

1. **Iniciar Sessão de Sombra**
    a. Faça login no Citrix Director
    b. navegar para a sessão do usuário que requer assistência
    c. Clique no botão "Sombra"
    d. Escolha Compartilhamento de Tela HDX
2. **Iniciar Visualizador**
    a. Abra o arquivo de incidente gerado com TWPlayer/Visualizador de Assistência Remota
    b. Aguarde o usuário aceitar a solicitação de conexão
3. **Visualizar Sessão**
    a. A tela da sessão aparece na janela do visualizador

b. O administrador pode observar as ações do usuário em tempo real

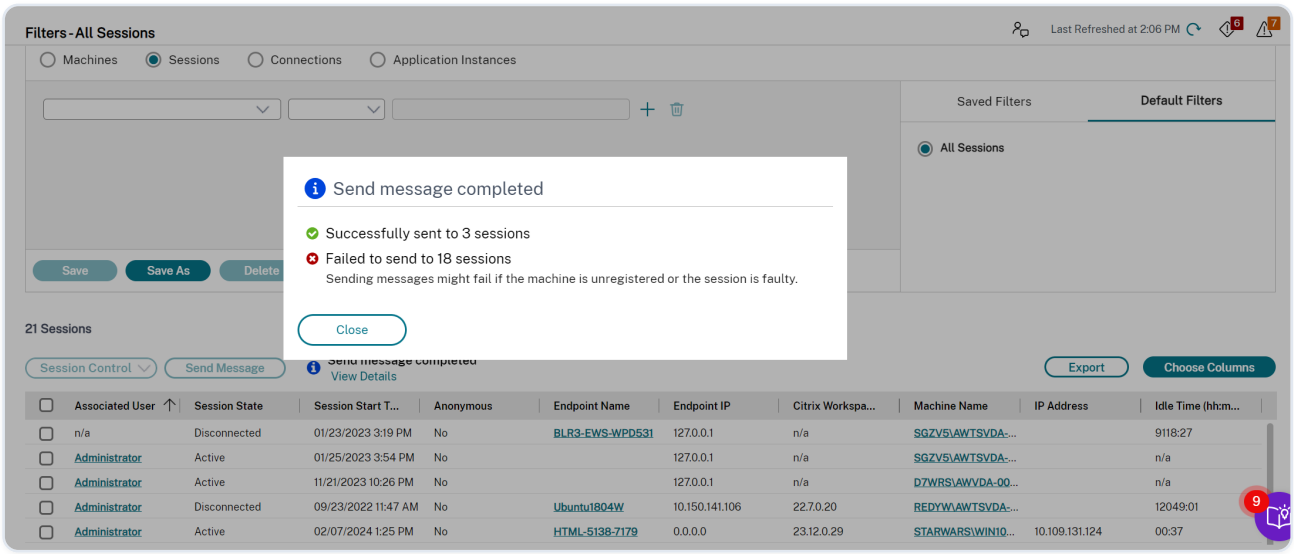


Enviar mensagens para usuários

No Monitor, envie uma mensagem para um usuário conectado a uma ou mais máquinas. Por exemplo, use esse recurso para enviar avisos imediatos sobre ações administrativas, como manutenção iminente da área de trabalho, logoffs e reinícios de máquinas e redefinições de perfil.

Para enviar uma mensagem a um usuário, siga estas etapas:

1. Vá para **Monitor** > **Filters** > **Machines** > **All Machines**.
2. Selecione uma máquina para a qual você deseja enviar uma mensagem e clique em **Send Message**.
3. Digite sua mensagem e clique em **Send**.



O envio de mensagens pode falhar se as máquinas não estiverem registradas ou se as sessões estiverem com problemas.

Se a mensagem for enviada com sucesso, uma mensagem de confirmação será exibida. Se a máquina do usuário estiver conectada, a mensagem aparecerá lá.

Se a mensagem não for enviada com sucesso, uma mensagem de erro será exibida. Solucione o problema de acordo com a mensagem de erro. Quando terminar, digite novamente o assunto e o texto da mensagem e clique em **Try again**.

Se você optar por enviar mensagens em massa para todas as sessões conectadas, o progresso da operação será exibido em porcentagem. Concluída a operação, o número de mensagens enviadas com sucesso e o número de mensagens que falharam serão exibidos. O status de envio de mensagens é particularmente útil ao administrar grandes sites. Ele ajuda a entender se a mensagem precisa ser reenviada a determinados usuários.

Função personalizada para limitar a opção de ação em massa para ações do usuário

Este recurso permite a adição de funções personalizadas para limitar o que o administrador pode ver e controlar. A nova função personalizada limita a capacidade de selecionar ações em massa, como logoff, desconexão ou mensagem. Esse controle é necessário para evitar ações em massa não intencionais ou maliciosas nos usuários.

Agora você pode editar funções para limitar as permissões de ação em massa usando as seguintes etapas:

1. Faça login no Citrix Cloud.
2. navegar até **Função** e selecione a função **Executar ações em massa não está habilitado**.
3. Clique nos três pontos e selecione **Editar**.
4. Vá para **Director > Gerenciar** e selecione a caixa de seleção **Executar ações em massa para ações de energia de máquinas, operações de modo de manutenção e gerenciamento de sessão**.
5. Certifique-se de que as seguintes funções também estejam selecionadas:

    - **Habilitar/desabilitar o modo de manutenção de uma máquina via Associação de Catálogo de Máquinas**
    - **Habilitar/desabilitar o modo de manutenção na área de trabalho via Associação de Catálogo de Máquinas**

- **Executar operações de energia em máquinas Windows Desktop via Associação de Catálogo de Máquinas**
- **Executar operações de energia em máquinas Windows Server via Associação de Catálogo de Máquinas**

Se as opções na etapa 5 forem selecionadas, o usuário poderá executar uma única ação. Para executar ações em massa, a opção na etapa 4 e as opções na etapa 5 devem ser selecionadas.

Resolver falhas de aplicativo

Na exibição do **Gerenciador de Atividades**, clique na guia **Aplicativos**. Você pode visualizar todos os aplicativos em todas as máquinas às quais este usuário tem acesso, incluindo aplicativos locais e hospedados para a máquina atualmente conectada, e o status de cada um.

A lista inclui apenas os aplicativos que foram iniciados dentro da sessão.

Para máquinas com SO de múltiplas sessões e máquinas com SO de sessão única, os aplicativos são listados para cada sessão desconectada. Se o usuário não estiver conectado, nenhum aplicativo será exibido.

AÇÃO	DESCRIÇÃO
Encerrar o aplicativo que não está respondendo	Escolha o aplicativo que não está respondendo e clique em **Encerrar Aplicativo**. Assim que o aplicativo for encerrado, peça ao usuário para iniciá-lo novamente.
Encerrar processos que não estão respondendo	Se você tiver a permissão necessária, clique na guia **Processos**. Selecione um processo que esteja relacionado ao aplicativo ou que esteja usando uma grande quantidade de recursos de CPU ou memória, e clique em **Encerrar Processo**. No entanto, se você não tiver a permissão necessária para encerrar o processo, a tentativa de encerrar um processo falhará.
Reiniciar a máquina do usuário	Apenas para máquinas com SO de sessão única, para a sessão selecionada, clique em **Reiniciar**. Alternativamente, na exibição Detalhes da Máquina, use os controles de energia para reiniciar ou desligar a máquina.

AÇÃO	DESCRIÇÃO
	Instrua o usuário a fazer logon novamente para que você possa verificar o aplicativo. Para máquinas com SO de múltiplas sessões, a opção de reinicialização não está disponível. Em vez disso, faça logoff do usuário e permita que o usuário faça logon novamente.
Colocar a máquina em modo de manutenção	Se a imagem da máquina precisar de manutenção, como um patch ou outras atualizações, coloque a máquina em modo de manutenção. Na exibição Detalhes da Máquina, clique em **Detalhes** e ative a opção de modo de manutenção. Encaminhe para o administrador apropriado.

Desabilitar a visibilidade de aplicativos em execução

Por padrão, o Gerenciador de Atividades exibe uma lista de todos os aplicativos em execução para a sessão de um usuário. Essas informações podem ser visualizadas por todos os administradores que têm acesso ao recurso Gerenciador de Atividades. Para funções de Administrador Delegado, isso inclui Administrador Completo, Administrador de grupo de entrega e Administrador de Help Desk.

Para proteger a privacidade dos usuários e dos aplicativos que eles estão executando, você pode desabilitar a guia Aplicativos para listar os aplicativos em execução. Para fazer isso, no VDA, modifique a chave do registro em HKEY_LOCAL_MACHINE\\Software\\Citrix\\Director\ \TaskManagerDataDisplayed. Por padrão, a chave é definida como 1. Altere o valor para 0, o que significa que as informações não são coletadas do VDA e, portanto, não são exibidas no Gerenciador de Atividades.

> **Aviso:**
>
> A edição incorreta do registro pode causar sérios problemas que podem exigir a reinstalação do seu sistema operacional. A Citrix® não pode garantir que os problemas resultantes do uso incorreto do Editor do Registro possam ser resolvidos. Use o Editor do Registro por sua conta e risco. Certifique-se de fazer backup do registro antes de editá-lo.

Restaurar conexões de desktop

No Monitor, verifique o status da conexão do usuário para a máquina atual na barra de título do usuário.

Se a conexão de desktop falhou, o erro que causou a falha é exibido e pode ajudar você a decidir como solucionar o problema.

AÇÃO	DESCRIÇÃO
Certifique-se de que a máquina não esteja no modo de manutenção	Na página Detalhes do Usuário, certifique-se de que o modo de manutenção esteja desativado.
Reiniciar a máquina do usuário	Selecione a máquina e clique em **Reiniciar**. Use esta opção se a máquina do usuário não estiver respondendo ou não conseguir se conectar, como quando a máquina está usando uma quantidade incomumente alta de recursos da CPU, o que pode tornar a CPU inutilizável.

Restaurar sessões

Se uma sessão for desconectada, ela ainda estará ativa e seus aplicativos continuarão a ser executados, mas o dispositivo do usuário não estará mais se comunicando com o servidor.

Na exibição Detalhes do Usuário, solucione falhas de sessão no painel **Detalhes da Sessão**. Você pode visualizar os detalhes da sessão atual, indicados pelo ID da sessão.

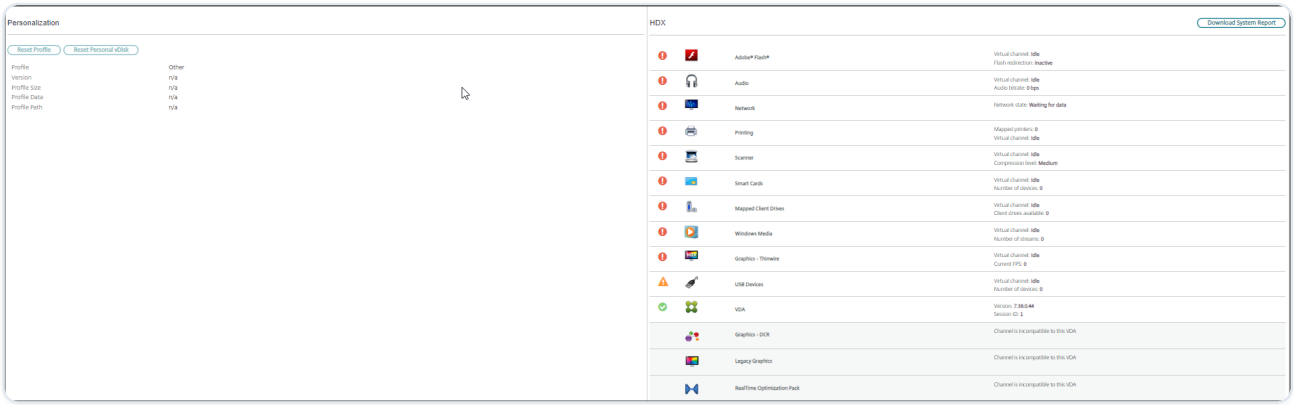
AÇÃO	DESCRIÇÃO
Encerrar aplicativos ou processos que não estão respondendo	Clique na guia **Aplicativos**. Selecione qualquer aplicativo que não esteja respondendo e clique em **Encerrar Aplicativo**. Da mesma forma, selecione qualquer processo correspondente que não esteja respondendo e clique em **Encerrar Processo**. Além disso, encerre processos que estão consumindo uma quantidade incomumente alta de memória ou recursos de CPU, o que pode tornar a CPU inutilizável.

AÇÃO	DESCRIÇÃO
Desconectar a sessão do Windows	Clique em **Controle de Sessão** e selecione **Desconectar**. Esta opção está disponível apenas para máquinas de SO multissessão intermediadas. Para sessões não intermediadas, a opção está desabilitada.
Fazer logoff do usuário da sessão	Clique em **Controle de Sessão** e selecione **Logoff**.

Para testar a sessão, o usuário pode tentar fazer logon novamente. Você também pode acompanhar o usuário para monitorar mais de perto esta sessão.

Gerar relatórios do sistema de canais HDX™

Na visualização de **Detalhes do Usuário**, verifique o status dos canais HDX na máquina do usuário no painel HDX. Este painel está disponível somente se a máquina do usuário estiver conectada usando HDX.



Se uma mensagem aparecer indicando que as informações não estão disponíveis no momento, aguarde um minuto para que a página seja atualizada ou selecione o botão **Atualizar**. Os dados HDX demoram um pouco mais para serem atualizados do que outros dados.

Clique em um ícone de erro ou aviso para obter mais informações.

> Dica:

> Você pode visualizar informações sobre outros canais na mesma caixa de diálogo clicando nas setas esquerda e direita no canto esquerdo da barra de título.

> Os relatórios do sistema de canais HDX são usados principalmente pelo Suporte Citrix para solucionar problemas. Para fazer isso, no painel HDX, clique em **Baixar Relatório do Sistema**.

Redefinir um perfil de usuário

> **Cuidado:**

> Quando um perfil é redefinido, embora as pastas e arquivos do usuário sejam salvos e copiados para o novo perfil, a maioria dos dados do perfil do usuário é excluída (por exemplo, o registro é redefinido e as configurações do aplicativo podem ser excluídas).

1. No Monitor, procure o usuário cujo perfil você deseja redefinir e selecione a sessão desse usuário.
2. Clique em **Redefinir Perfil**.
3. Instrua o usuário a fazer logoff de todas as sessões.
4. Instrua o usuário a fazer logon novamente. As pastas e arquivos que foram salvos do perfil do usuário são copiados para o novo perfil.

   > **Importante:**

   > Se o usuário tiver perfis em várias plataformas (como Windows 8 e Windows 7), instrua-o a fazer logon novamente primeiro no mesmo desktop ou aplicativo que ele relatou como problema. Isso garante que o perfil correto seja redefinido. Para um perfil de usuário Citrix®, o perfil já é redefinido no momento em que a área de trabalho do usuário aparece. Para um perfil móvel da Microsoft, a restauração da pasta ainda pode estar em andamento por um breve período. O usuário deve permanecer conectado até que a restauração seja concluída.

As etapas anteriores pressupõem que você esteja usando o Citrix Virtual Desktops™ (VDA de Desktop). Se você estiver usando o Citrix Virtual Desktops (VDA de Servidor), precisará estar conectado para realizar a redefinição do perfil. O usuário precisará então fazer logoff e logon novamente para concluir a redefinição do perfil.

Se o perfil não for redefinido com sucesso (por exemplo, o usuário não conseguir fazer logon novamente na máquina ou alguns arquivos estiverem faltando), você deverá restaurar manualmente o perfil original.

As pastas (e seus arquivos) do perfil do usuário são salvas e copiadas para o novo perfil. Elas são copiadas na ordem listada:

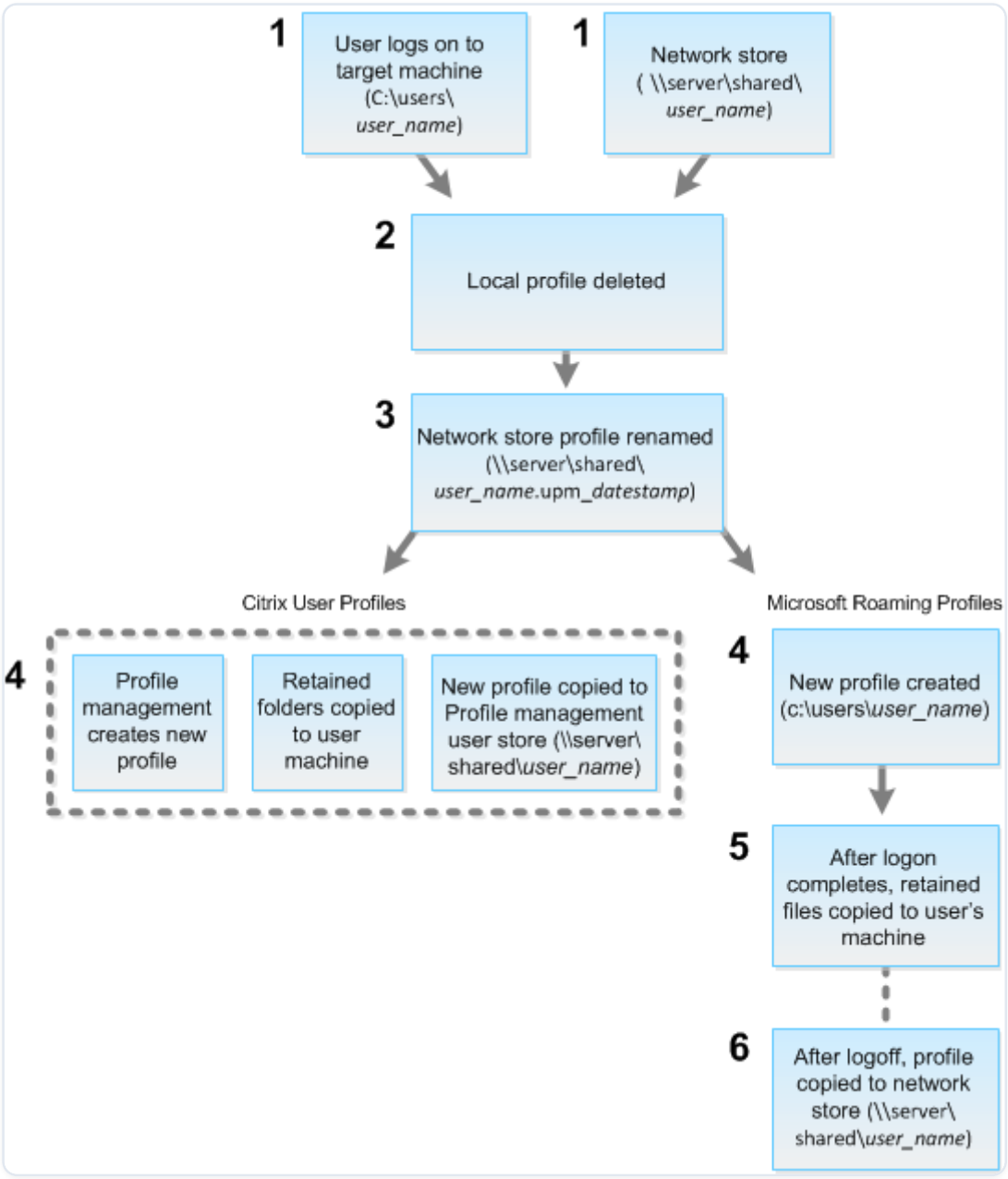
- Área de Trabalho
- Cookies
- Favoritos
- Documentos
- Imagens
- Música
- Vídeos

> **Nota:**
>
> No Windows 8 e posterior, os cookies não são copiados quando os perfis são redefinidos.

Como os perfis redefinidos são processados

Qualquer perfil de usuário Citrix ou perfil móvel da Microsoft pode ser redefinido. Depois que o usuário faz logoff e você seleciona o comando de redefinição (seja no Monitor ou usando o SDK do PowerShell), o Monitor primeiro identifica o perfil de usuário em uso e emite um comando de redefinição apropriado. O Monitor recebe as informações através do Profile Management, incluindo informações sobre o tamanho, tipo e tempos de logon do perfil.

Este diagrama ilustra o processo após o logon do usuário, quando um perfil de usuário é redefinido.



O comando de redefinição emitido pelo Monitor especifica o tipo de perfil. O serviço Profile Management então tenta redefinir um perfil desse tipo e procura o compartilhamento de rede apropriado (repositório de usuário). Se o Profile Management processar o usuário, mas receber um comando de perfil móvel, ele será rejeitado (ou vice-versa).

1. Se um perfil local estiver presente, ele é excluído.
2. O perfil de rede é renomeado.
3. A próxima ação depende se o perfil que está sendo redefinido é um perfil de usuário Citrix ou um perfil móvel da Microsoft.

   Para perfis de usuário Citrix, o novo perfil é criado usando as regras de importação do Profile Management, e as pastas são copiadas de volta para o perfil de rede, e o usuário pode fazer logon normalmente. Se um perfil móvel for usado para a redefinição, quaisquer configurações

de registro no perfil móvel serão preservadas no perfil redefinido. Você pode configurar o Profile Management para que um perfil de modelo substitua o perfil móvel, se necessário.

Para perfis móveis da Microsoft, o Windows cria um novo perfil e, quando o usuário faz logon, as pastas são copiadas de volta para o dispositivo do usuário. Quando o usuário faz logoff novamente, o novo perfil é copiado para o armazenamento de rede.

Para restaurar manualmente um perfil após uma redefinição com falha

1. Instrua o usuário a fazer logoff de todas as sessões.
2. Exclua o perfil local, se existir.
3. Localize a pasta arquivada no compartilhamento de rede que contém a data e a hora anexadas ao nome da pasta, a pasta com uma extensão .upm_datestamp.
4. Exclua o nome do perfil atual. Ou seja, aquele sem a extensão upm_datestamp.
5. Renomeie a pasta arquivada usando o nome do perfil original. Ou seja, remova a extensão de data e hora. Você retornou o perfil ao seu estado original, antes da redefinição.

Gravar sessões

Você pode gravar sessões ICA® usando os controles de Gravação de Sessão nas telas **Detalhes do Usuário** e **Detalhes da Máquina** no Director. Este recurso está disponível para clientes em sites **Premium**.

Gravação Dinâmica de Sessão

Você pode gravar a sessão ativa atual usando os controles de Gravação de Sessão na tela **Detalhes do Usuário**. Para obter mais informações sobre a Gravação Dinâmica de Sessão, consulte o artigo serviço de Gravação de Sessão.

Gravação de Sessão baseada em Política

Para configurar a Gravação de Sessão baseada em Política no Director usando a ferramenta DirectorConfig, consulte a seção **Configurar o Director para usar o Servidor de Gravação de Sessão** em Configurar políticas de gravação de sessão. Os controles de Gravação de Sessão estão disponíveis no Director somente se o usuário logado tiver permissão para modificar as políticas de Gravação de Sessão. Essa permissão pode ser definida no console de Autorização de Gravação de Sessão, conforme descrito em Autorizar usuários.

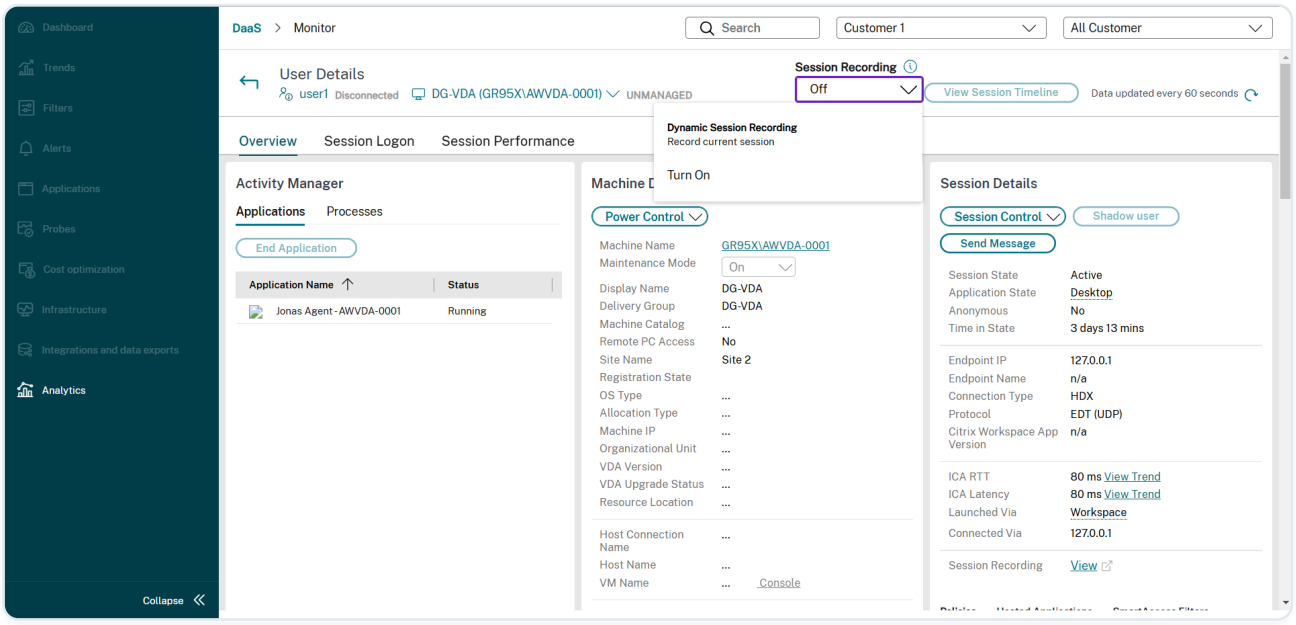
> **Nota:** As alterações feitas nas configurações de Gravação de Sessão através do Director ou do console de Política de Gravação de Sessão entram em vigor a partir da sessão ICA subsequente.

Controles de Gravação de Sessão no Director

Você pode usar as ações **Detalhes do Usuário** > **Gravação de Sessão** para gravar as sessões atuais ou subsequentes.

- Ativar Gravação Dinâmica de Sessão - a sessão atual é gravada.
- Ativar (com notificação) - as sessões subsequentes são gravadas e o usuário é notificado sobre a gravação da sessão ao fazer logon na sessão ICA.
- Ativar (sem notificação) - as sessões subsequentes são gravadas e a sessão é gravada silenciosamente sem notificar o usuário.
- Desativar - desabilita a gravação de sessões para o usuário.

O Painel **Políticas** exibe o nome da política de Gravação de Sessão ativa.



O painel **Detalhes da Máquina** exibe o status da política de Gravação de Sessão para a máquina.

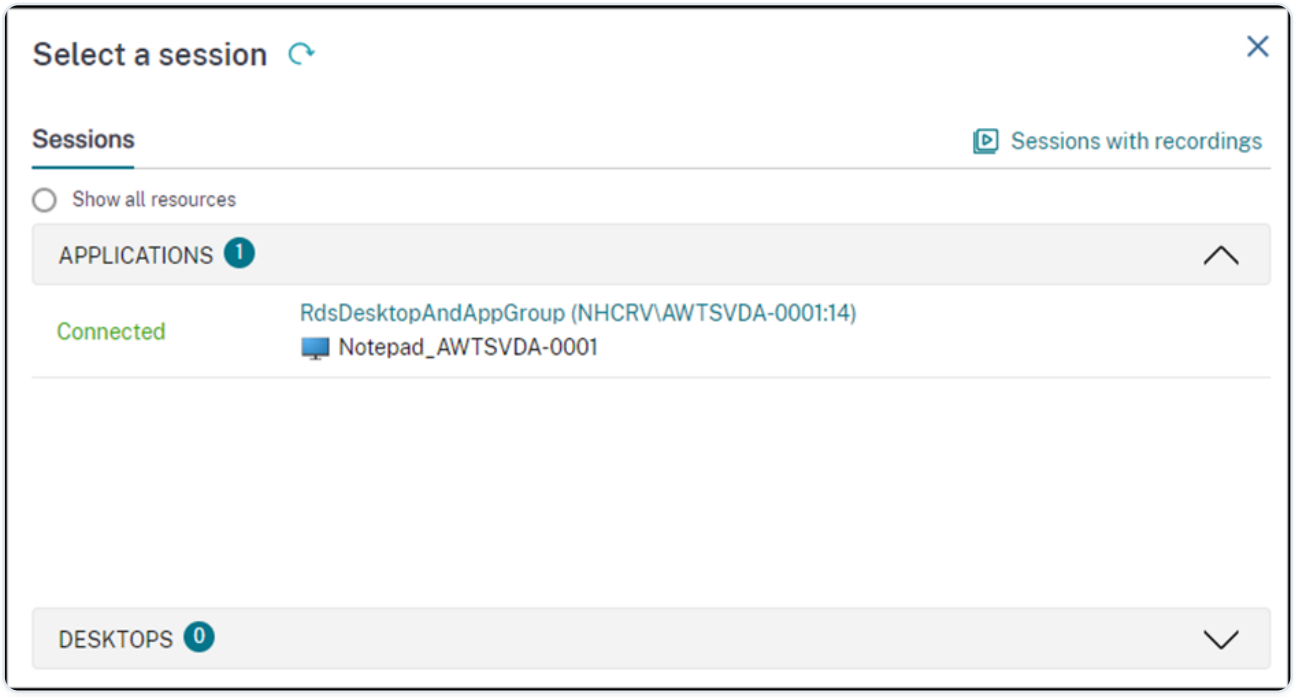
REPRODUZIR SESSÕES AO VIVO E GRAVADAS

Você pode reproduzir sessões de usuário gravadas e ao vivo para entender os problemas encontrados pelo usuário. O acesso fácil a gravações e métricas relacionadas à sessão dentro do console do Director elimina a necessidade de procurar as gravações em vários servidores de gravação de sessão ou de procurar aplicativos de terceiros para visualizar as gravações. Isso ajuda a correlacionar os problemas descobertos nas gravações com as métricas de desempenho.

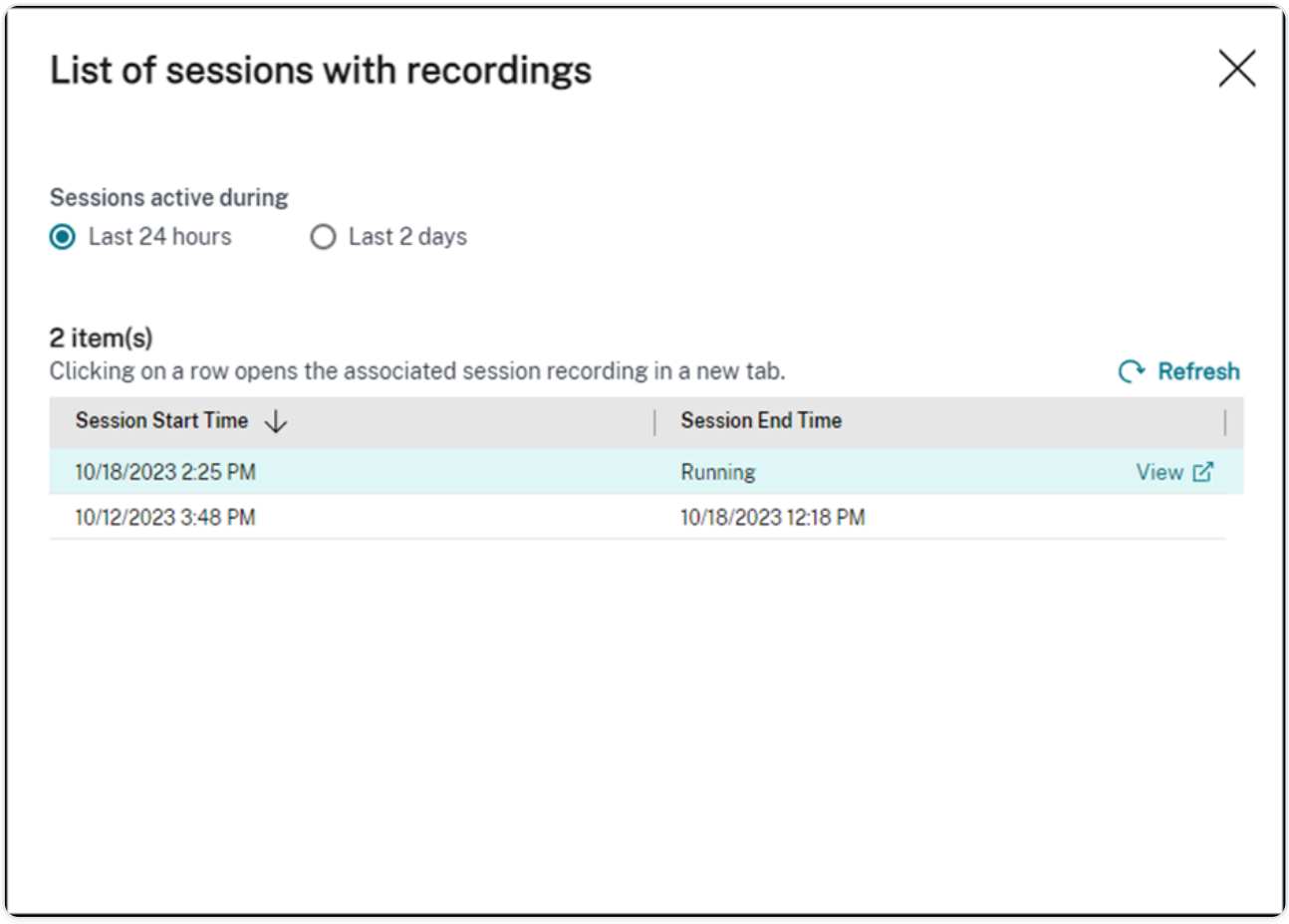
Este recurso requer o seguinte:

- O VDA e os servidores de Gravação de Sessão estão na versão 2308 ou posterior.
- O Delivery Controller™ e o Director estão na versão 2311 ou posterior.

O Director armazena as gravações de sessão em um repositório centralizado. A lista de gravações pertencentes ao usuário é exibida ao clicar no link **Sessões com gravações** no modal **Seletor de Sessão**.



Você pode optar por visualizar gravações de sessões que estiveram ativas nas últimas 24 horas ou nos últimos 2 dias. As gravações ao vivo de sessões atualmente ativas são marcadas com **Hora de Término da Sessão** como **Em Execução**.



Clique no link **Visualizar** para reproduzir a gravação em uma nova guia usando o servidor de reprodução do Citrix Session Recording.

Solucionar problemas de máquinas

> **Nota:**

> O **Citrix Health Assistant** é uma ferramenta para solucionar problemas de configuração em VDAs não registrados. A ferramenta automatiza várias verificações de integridade para identificar possíveis causas raiz para falhas de registro de VDA e problemas no lançamento de sessão e na configuração de redirecionamento de fuso horário. O artigo da Central de Conhecimento, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch contém o download da ferramenta **Citrix Health Assistant** e as instruções de uso.

> A exibição **Filtros \> Máquinas** na guia Monitor exibe as máquinas configuradas no site. A guia Máquinas de SO de Múltiplas Sessões inclui o índice do avaliador de carga, que indica a distribuição de contadores de desempenho e dicas de ferramentas da contagem de sessões se você passar o mouse sobre o link.

Clique na coluna **Motivo da Falha** de uma máquina com falha para obter uma descrição detalhada da falha e as ações recomendadas para solucionar o problema. Os motivos da falha e as ações recomendadas para falhas de máquina e conexão estão disponíveis no Guia de Solução de Problemas de Motivos de Falha do Citrix Director.

Clique no link do nome da máquina para ir para a página **Detalhes da Máquina**.

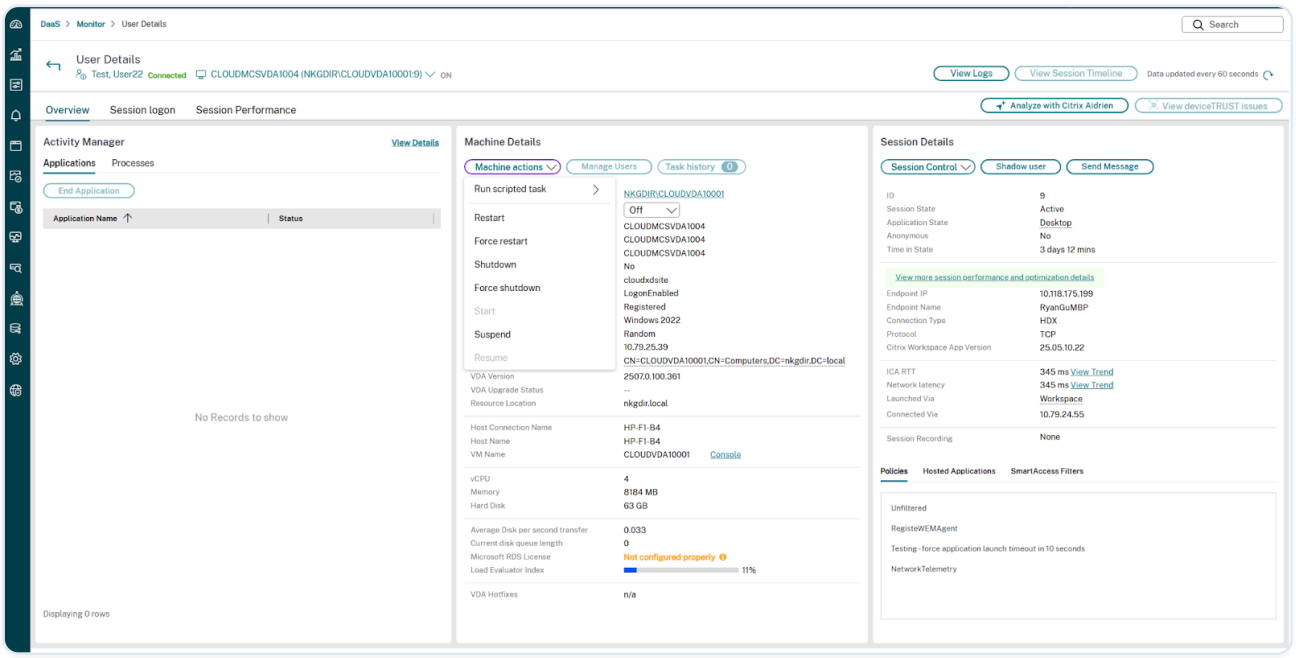
A página Detalhes da Máquina lista os detalhes da máquina, detalhes da infraestrutura e detalhes dos hotfixes aplicados na máquina.

Suporte para HDX™ Plus para PCs em Nuvem do Windows 365 e Desktops Virtuais do Azure:

> **Nota:**
>
> Para HDX Plus para PCs em Nuvem do Windows 365, apenas as opções de Controle de Energia Reiniciar e Forçar Reinício estão disponíveis. Para Desktops Virtuais do Azure (AVD), todas as opções de Controle de Energia estão disponíveis.

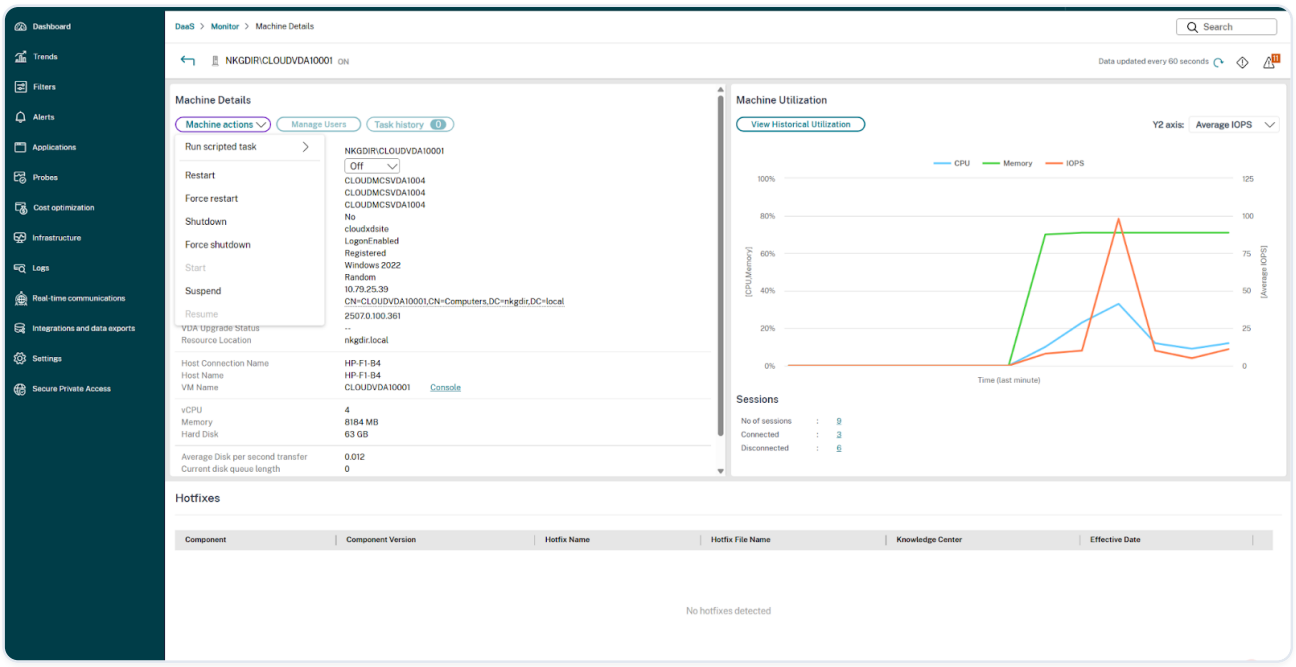
> Você pode visualizar as opções de Controle de Energia disponíveis usando um dos seguintes métodos:

Clique em **Filtros** > **Sessões** > **Detalhes da Máquina** > lista suspensa **Ações da máquina** e selecione uma opção para atribuir o controle de energia necessário ou a opção de tarefa script para uma máquina.



Ou,

Clique em **Filtros** > **Máquina** > **Detalhes da Máquina** > lista suspensa **Ações da máquina** e selecione uma opção para atribuir o controle de energia necessário ou a opção de tarefa script para uma máquina.



Nota:

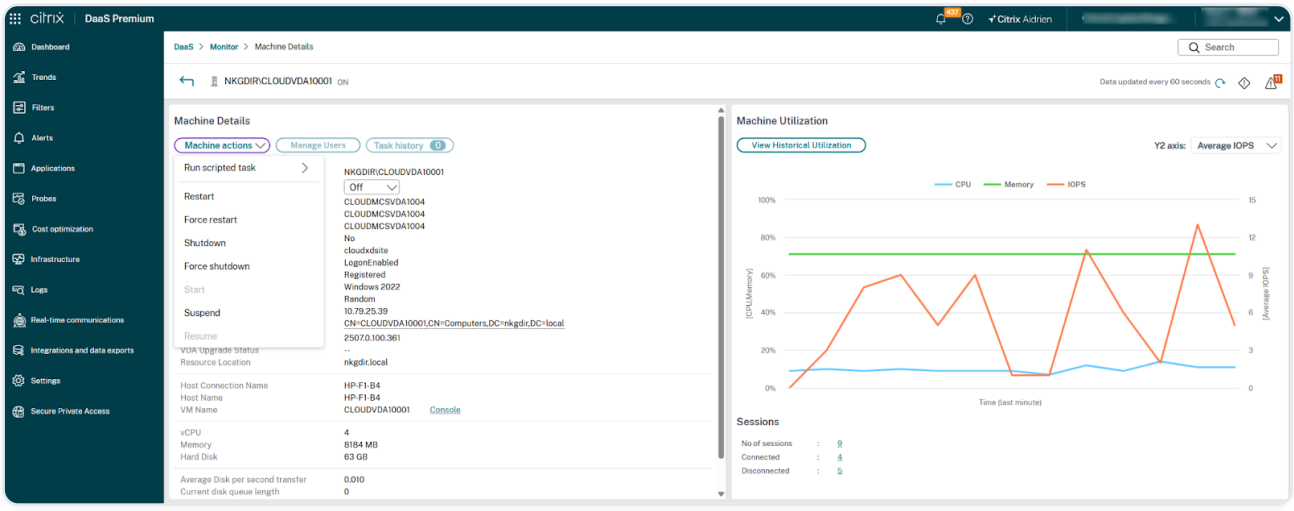
- A Execução de Tarefa de Script é suportada apenas quando o serviço WEM (Workspace Environment Management) é provisionado e o agente WEM no VDA está instalado e registrado com o serviço WEM.
- O Histórico de Tarefas mostra apenas as execuções de Tarefas de Script do usuário atual nas últimas 24 horas.

Utilização de recursos em tempo real baseada em máquina

O painel **Utilização da Máquina** exibe gráficos mostrando a utilização em tempo real da CPU e da memória. Além disso, gráficos de monitoramento de disco e GPU estão disponíveis para sites com versões de VDA 7.14 e posteriores.

Gráficos de monitoramento de disco, IOPS médio e latência do disco são medidas de desempenho importantes que ajudam você a monitorar e solucionar problemas relacionados aos discos VDA. O gráfico de IOPS Médio exibe o número médio de leituras e gravações em um

disco. Selecione **Latência do Disco** para ver um gráfico do atraso entre uma solicitação de dados e seu retorno do disco, medido em milissegundos.



UTILIZAÇÃO DA GPU

Selecione **Utilização da GPU** para ver a porcentagem de utilização da GPU, da memória da GPU e do Codificador e Decodificador para solucionar problemas relacionados à GPU em VDAs de SO de sessão múltipla e sessão única.

Versões de GPU suportadas:

- GPUs NVIDIA Tesla M60 executando a versão 369.17 ou posterior do Driver de Vídeo. Para obter mais informações, consulte NVIDIA vGPU Software.
- GPUs AMD Radeon Instinct MI25 e CPUs AMD EPYC 7V12 (Rome). Para obter mais informações, consulte AMD Drivers and Support.

Drivers:

Os drivers ou extensões apropriados devem ser instalados nos VDAs.

- Para GPUs NVIDIA, instale os drivers GRID manualmente ou via extensões. Para mais informações, consulte NVIDIA vGPU Software.
  - Observe que, para NVIDIA, apenas os drivers GRID são suportados. Os drivers CUDA não funcionam com a série NVadsA10 v5 e não são suportados.
  - Para um processo de exemplo para instalar drivers de GPU Nvidia Grid via extensões em máquinas baseadas no Azure, consulte NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
  - Para um processo de exemplo para instalar drivers de GPU Nvidia Grid manualmente, consulte Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines.

- Para GPUs AMD, instale os drivers gráficos AMD manualmente ou via extensões. Para mais informações, consulte AMD Drivers and Support.
    - Para um processo de exemplo para instalar drivers de GPU AMD via extensões em máquinas baseadas no Azure, consulte AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
    - Para um processo de exemplo para instalar drivers de GPU AMD manualmente em máquinas Azure, consulte Install AMD GPU drivers on N-series VMs running Windows.

Notas de Uso:

- Os gráficos de Utilização da GPU estão disponíveis apenas para VDAs executando Windows de 64 bits.
- Os gráficos de Utilização da GPU AMD estão disponíveis apenas para VDAs executando Citrix Virtual Apps and Desktops™ 7 2212 ou posterior.
- Os VDAs devem ter o HDX 3D Pro habilitado para fornecer aceleração de GPU. Para mais informações, consulte GPU acceleration for Windows Single-session OS e GPU acceleration for Windows Multi-session OS.
- Quando um VDA acessa mais de uma GPU, o gráfico de utilização exibe a média das métricas de GPU coletadas das GPUs individuais. As métricas de GPU são coletadas para todo o VDA e não para processos individuais.
- Para AMD, o uso do codificador e decodificador não é suportado separadamente. Qualquer carga de trabalho de codificação/decodificação usando a GPU será relatada como a carga 3D geral no uso da GPU.
- Certifique-se de instalar o NVIDIA WMI durante a instalação. Esta janela está disponível apenas durante a instalação manual.
- Se os drivers estiverem instalados, mas o Director não detectar a GPU
    - Verifique o Gerenciador de Tarefas. Se os drivers estiverem instalados corretamente, a GPU deverá aparecer no Gerenciador de Tarefas.
    - Verifique se a máquina está registrada. Às vezes, as máquinas podem levar algum tempo para serem detectadas como online.
- Se o uso da GPU não mostrar atividade no Director, certifique-se de que a carga de trabalho que você está executando esteja usando a GPU. Para cargas de trabalho gráficas, isso pode ser ativado em Configurações > Sistema > Tela > Configurações de gráficos > Escolher o aplicativo para definir a preferência. Certifique-se de ativar o Alto Desempenho. Às vezes, o

Windows usa a CPU por padrão para cargas de trabalho gráficas quando isso é definido como padrão do sistema ou economia de energia, com base em outras configurações.

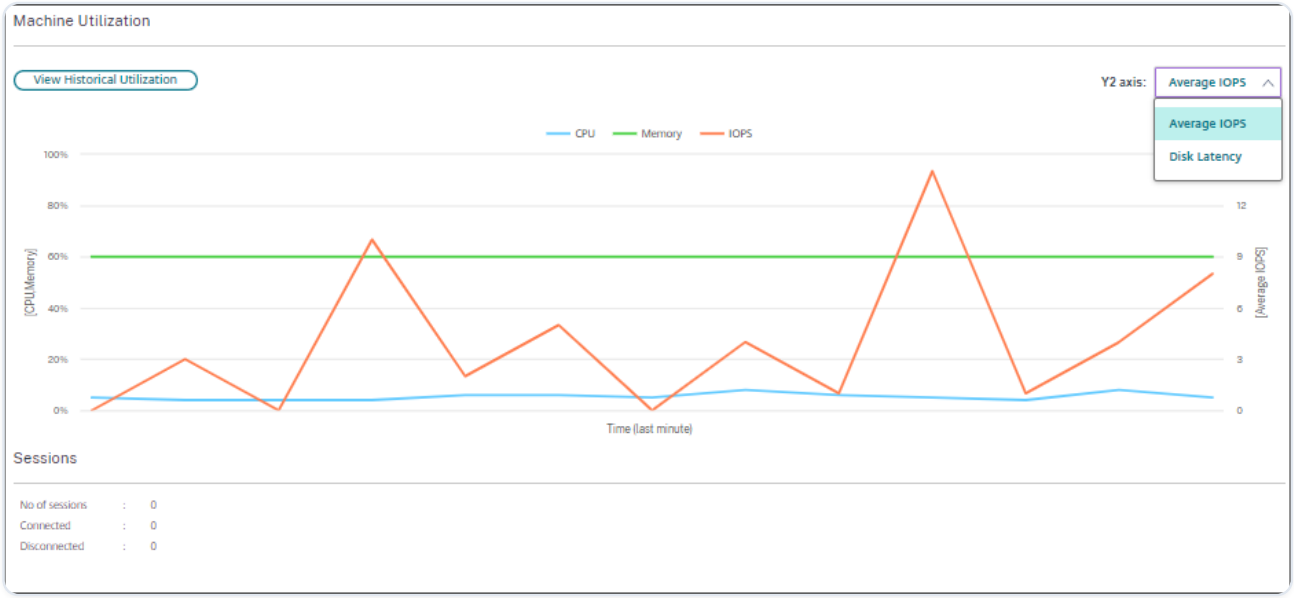
- Os dados são atualizados a cada minuto e a visualização dos dados começa em um minuto após a seleção de **Utilização da GPU**.

Utilização histórica de recursos baseada em máquina

No painel **Utilização da Máquina**, clique em **Exibir Utilização Histórica** para ver o uso histórico de recursos na máquina selecionada. Os gráficos de utilização incluem contadores de desempenho críticos de CPU, memória, sessões simultâneas de pico, IOPS médio e latência de disco.

> **Nota:**
>
> A configuração da política de Monitoramento, **Habilitar Monitoramento de Processos**, deve ser definida como Permitido para coletar e exibir dados na tabela dos 10 Principais Processos na página de Utilização Histórica da Máquina. A coleta é proibida por padrão.

> Os dados de utilização de CPU e memória, IOPS médio e latência de disco são coletados por padrão. Você pode desabilitar a coleta usando a configuração da política **Habilitar Monitoramento de Recursos**.

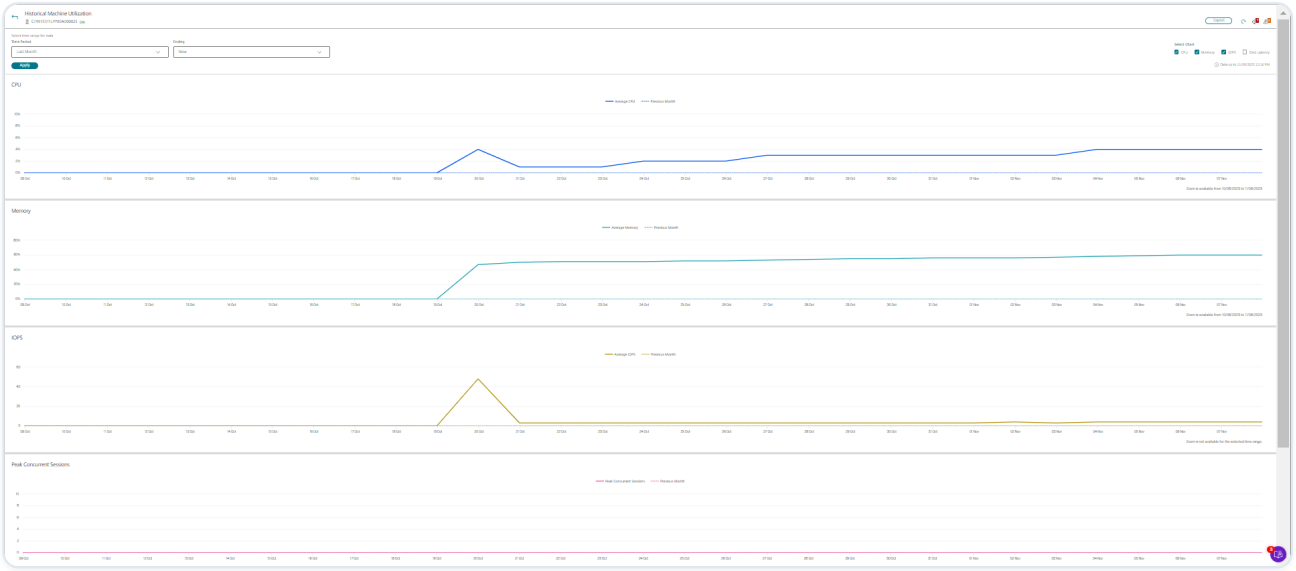


1. No painel **Utilização da Máquina** na visualização **Detalhes da Máquina**, selecione **Exibir Utilização Histórica**.
2. Na página **Utilização Histórica da Máquina**, defina o **Período de Tempo** para visualizar o uso das últimas 2 horas, 24 horas, 7 dias, mês ou ano.

Nota:

Os dados de uso de IOPS médio e latência de disco estão disponíveis apenas para as últimas 24 horas, mês e ano terminando agora. Horário de término personalizado não é suportado.

3. Clique em **Aplicar** e selecione os gráficos necessários.
4. Passe o mouse sobre as diferentes seções do gráfico para ver mais informações para o período de tempo selecionado.



Por exemplo, se você selecionar **Últimas 2 horas**, o período de linha de base é as 2 horas anteriores ao intervalo de tempo selecionado. Visualize a tendência de CPU, memória e sessão nas últimas 2 horas e no tempo de linha de base. Se você selecionar **Último mês**, o período de linha de base é o mês anterior. Selecione para visualizar a média de IOPS e a latência de disco no último mês e no tempo de linha de base.

1. Clique em **Exportar** para exportar os dados de utilização de recursos para o período selecionado. Para obter mais informações, consulte a seção Exportar relatórios em Monitorar Implantações.
2. Abaixo dos gráficos, a tabela lista os 10 principais processos com base na utilização da CPU ou da memória. Você pode classificar por qualquer uma das colunas, que mostram Nome do Aplicativo, Nome de Usuário, ID da Sessão, CPU Média, Pico de CPU, Memória Média e Pico de Memória no intervalo de tempo selecionado. As colunas IOPS e Latência de Disco não podem ser classificadas.

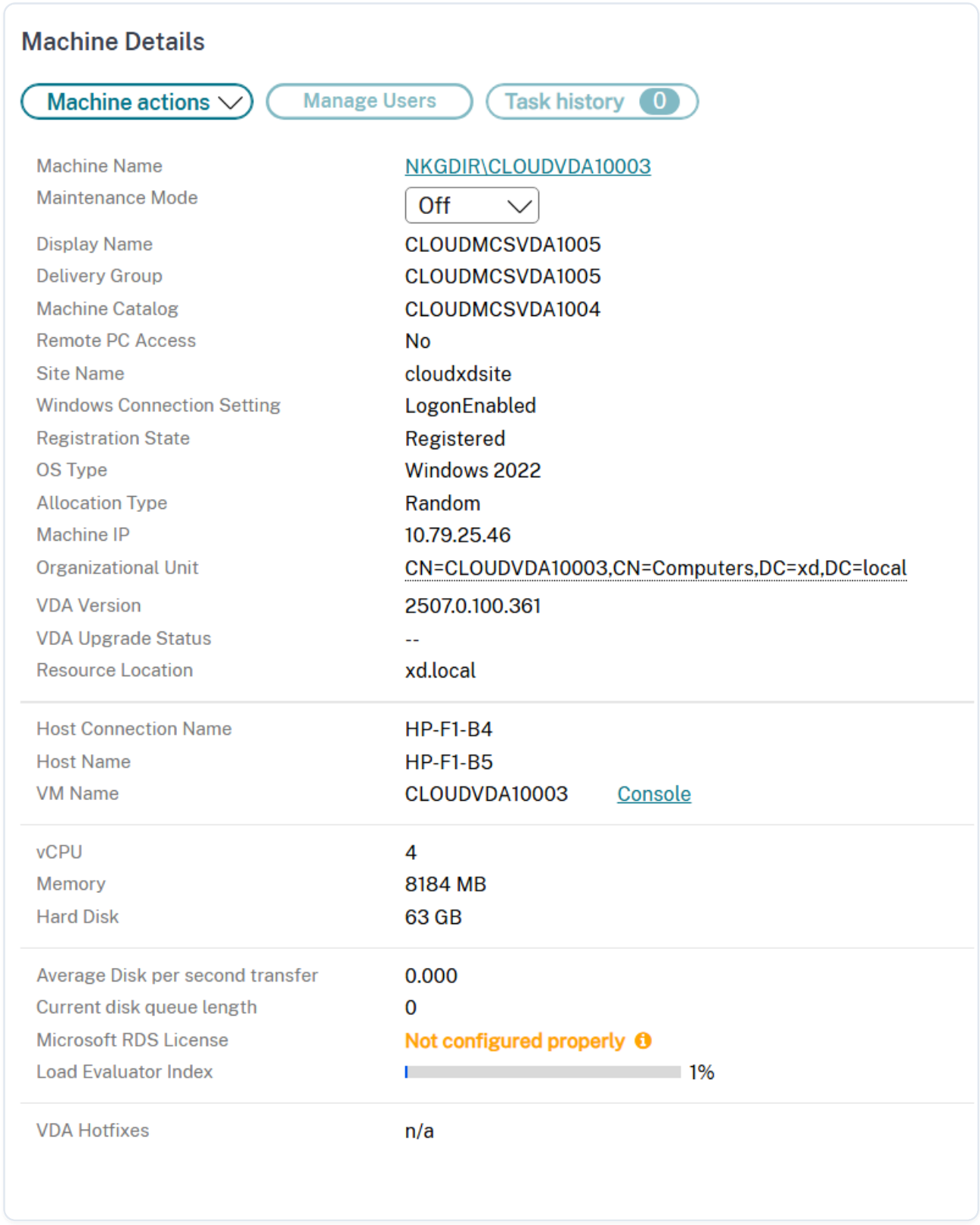
Nota:

- O ID da sessão para processos do sistema é exibido como "0000".
- Se um site que pertence ao plano Citrix Cloud™ Japan ou Citrix Cloud Government contiver mais de 5000 máquinas, os dados do processo estarão disponíveis para até 2000 máquinas apenas. A política de Monitoramento de Processos deve ser habilitada nessas máquinas.

3. Para visualizar a tendência histórica do consumo de recursos de um processo específico, detalhe qualquer um dos 10 principais processos.

Acesso ao console da máquina

Você pode acessar os consoles de máquinas Desktop e Multi-session OS hospedadas no XenServer Versão 7.3 e posterior diretamente do Monitor. Dessa forma, você não precisa do XenCenter para solucionar problemas em VDAs hospedados no XenServer. Para que esse recurso esteja disponível, o XenServer que hospeda a máquina deve ser da Versão 7.3 ou posterior e deve estar acessível a partir do Monitor.



Para solucionar problemas em uma máquina, clique no link **Console** no painel Detalhes da Máquina correspondente. Após a autenticação das credenciais do host que você fornece, o console da máquina é aberto em uma nova guia usando o noVNC, um cliente VNC baseado na web. Agora você tem acesso ao console com teclado e mouse.

Nota:

- Este recurso não é compatível com o Internet Explorer 11.
- Se o ponteiro do mouse no console da máquina estiver desalinhado, consulte CTX230727 para obter as etapas para corrigir o problema.
- O acesso ao console é iniciado em uma nova guia, certifique-se de que as configurações do seu navegador permitam pop-ups.
- Por motivos de segurança, a Citrix® recomenda que você instale certificados SSL em seu navegador.

Inspecionar máquinas com ações de energia recentes

Agora você pode inspecionar máquinas com o status das ações de energia bem-sucedidas e falhas. Este recurso ajuda você a analisar o seguinte:

- Falha ao ligar que causa problemas ao usuário
- Falha ao desligar que aumenta o custo

Nota:

Os dados estão disponíveis apenas para a máquina gerenciada por energia. Os dados não estão disponíveis para as ações de energia realizadas antes que o recurso fosse suportado.

Você pode visualizar o status da ação de energia das máquinas usando as seguintes formas:

Na guia **Filtros** -> **Máquinas**. Nesse caso, por padrão, as colunas **Hora da Ação de Energia** e **Resultado da Ação de Energia** ficam visíveis. Você também pode selecionar as colunas que deseja que fiquem visíveis.

Na guia **Otimização de Custos**. Nesse caso, o filtro padrão **Ação de Energia Acionada Por** é definido como *Autoscale*™ e o **Resultado da Ação de Energia** é definido como *Falha*.

Com este recurso, você pode visualizar os detalhes dos controles de ação de energia. Por exemplo, você pode visualizar quem acionou a ação, qual ação alterou o estado de energia, o motivo da falha e a hora em que a ação foi concluída. Você também pode exportar esses detalhes.

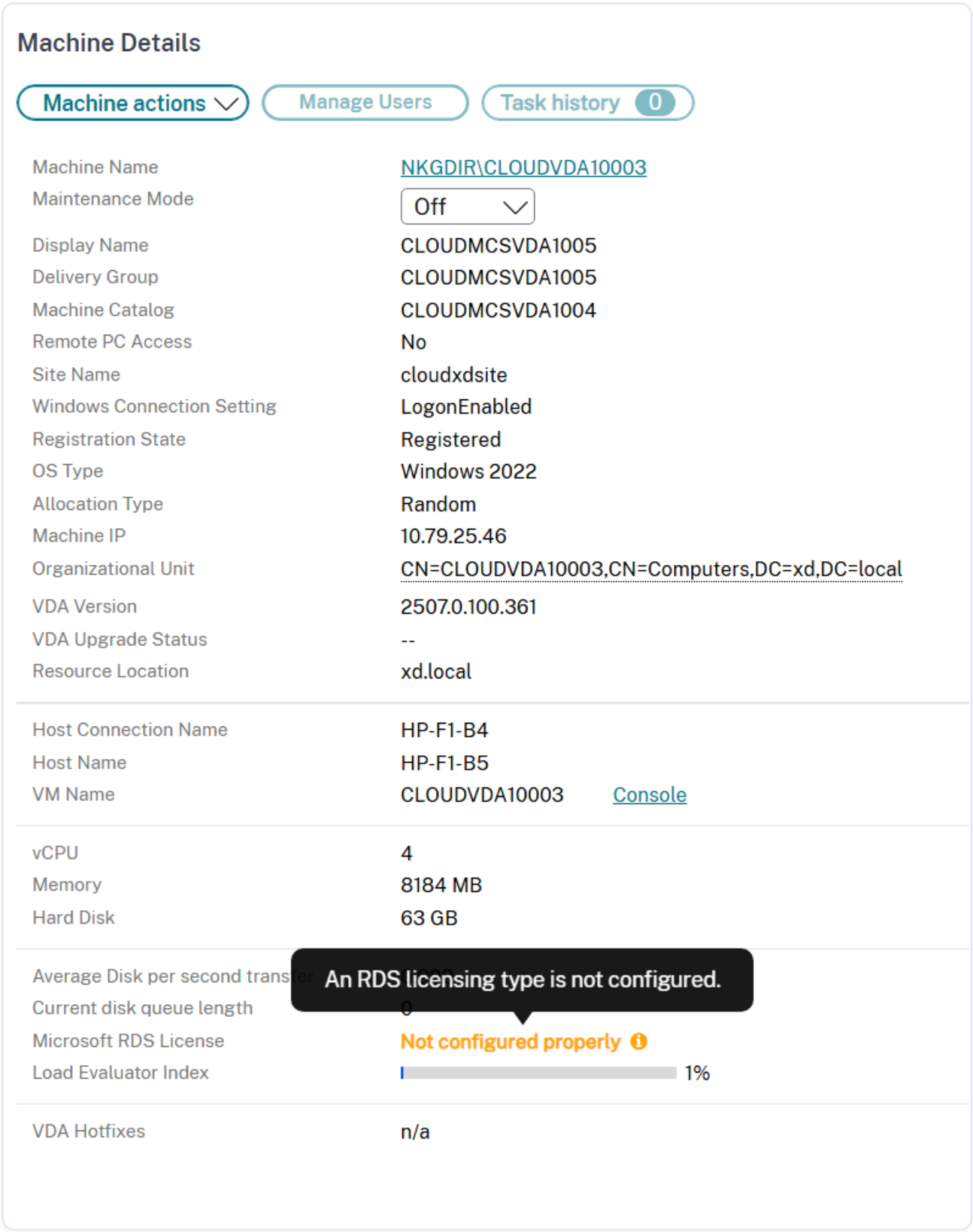
Os seguintes filtros são adicionados para visualizar o status da ação de energia:

FILTRO	DESCRIÇÃO
Resultado da Ação de Energia	Exibe o resultado da ação de energia. Os valores de filtro possíveis são sucesso e falha.
Ação de Energia Acionada Por	Exibe quem ou o que acionou a ação de energia. Os valores de filtro possíveis são os seguintes • Autoscale - Este valor aparece quando uma ação de energia é acionada pelo seguinte • Quando o administrador desliga uma VM para limpar o disco do SO da VM de volta ao seu estado inicial • Quando uma VM é desligada ou suspensa com base nas políticas definidas • Quando uma VM é disponibilizada com base no tamanho do pool ou na configuração do tamanho do buffer • Administrador - Este valor aparece quando uma ação de energia é acionada por um administrador. Os exemplos possíveis são quando o administrador solicita desligar, ligar, suspender, retomar, reiniciar ou reinicializar uma VM.

FILTRO	DESCRIÇÃO
	• Usuário - Este valor aparece quando uma ação de energia é acionada por um usuário. Os exemplos são quando um usuário redefine, liga ou retoma o trabalho na VM.
	• Outros - Este valor aparece quando uma ação de energia é acionada por motivos agendados e desconhecidos.
Última Ação de Energia	Exibe a ação de energia exata que ocorreu na máquina, como ligar, desligar, encerrar, reiniciar, redefinir, retomar e assim por diante
Hora da Ação de Energia	A hora em que a ação de energia é concluída. Os possíveis valores de filtro são último minuto, últimos 5 minutos, últimos 30 minutos, última hora, hoje, últimas 24 horas e ontem.
Motivo da Falha da Ação de Energia	Exibe o motivo da falha. Os possíveis valores de filtro são falha relatada pelo hipervisor, limite de taxa do hipervisor excedido, erro desconhecido e nenhum. Se houver uma ação bem-sucedida, ele mostra "Nenhum".

Integridade da licença do Microsoft RDS

Você pode visualizar o status da licença do Microsoft RDS no painel Detalhes da Máquina nas páginas **Detalhes da Máquina** e **Detalhes do Usuário** para máquinas Multi-session OS.



Uma das seguintes mensagens é exibida:

- Licença disponível
- Não configurado corretamente (aviso)
- Erro de licença (erro)

- Versão VDA incompatível (erro)

Nota:

O status de integridade da licença Microsoft RDS para máquinas em período de carência com licença válida exibe uma mensagem de **Licença disponível** em verde. Renove sua licença antes que ela expire.

Para mensagens de aviso e erro, passe o mouse sobre o ícone de informações para visualizar detalhes adicionais, conforme a tabela a seguir.

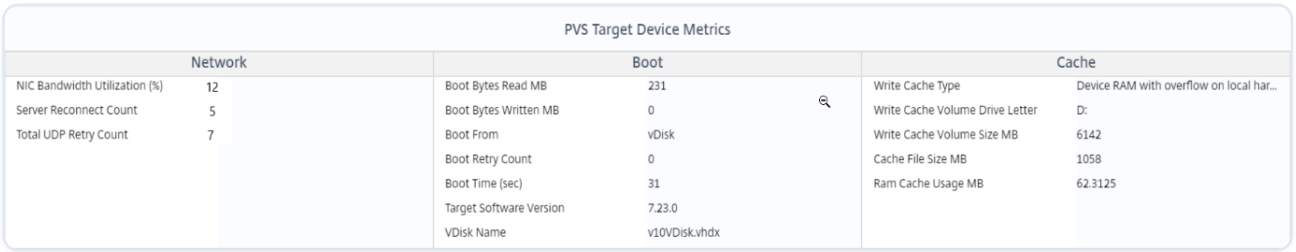
TIPO DE MENSAGEM	MENSAGENS NO MONITOR
Erro	Disponível para VDAs versão 7.16 e posterior.
Erro	Novas conexões RDS não são permitidas.
Erro	A licença Microsoft RDS excedeu seu período de carência.
Erro	Um Servidor de Licenças não está configurado para o nível de SO exigido com o tipo de licenciamento de Acesso de Cliente Por Dispositivo.
Erro	O Servidor de Licenças configurado é incompatível com o nível de SO do Host RDS com o tipo de licenciamento de Acesso de Cliente Por Dispositivo.
Aviso	O Servidor de Terminal Pessoal não é um tipo de licenciamento RDS válido em uma implantação do Citrix Virtual Apps and Desktops.
Aviso	A Área de Trabalho Remota para Administração não é um tipo de licenciamento válido em uma implantação do Citrix Virtual Apps and Desktops.

TIPO DE MENSAGEM	MENSAGENS NO MONITOR
Aviso	Um tipo de licenciamento RDS não está configurado.
Aviso	O Controlador de Domínio ou Servidor de Licenças está inacessível com o tipo de licenciamento RDS de Acesso de Cliente Por Usuário.
Aviso	Com o tipo de licenciamento de Acesso de Cliente Por Dispositivo, a licença do Dispositivo Cliente não pôde ser determinada, pois o servidor de licenças para o nível de SO exigido está inacessível.

> **Nota:**
>
> Este recurso é aplicável apenas para CAL RDS da Microsoft (Licença de Acesso de Cliente).

Métricas de dispositivo de destino PVS

Você pode visualizar o status dos dispositivos de destino PVS para máquinas de SO de sessão única e multi-sessão na página **Detalhes da Máquina** no Monitor. Várias métricas para **Rede**, **Inicialização** e **Cache** estão disponíveis neste painel. Essas métricas ajudam você a monitorar e solucionar problemas de dispositivos de destino PVS para garantir que estejam em funcionamento.



Rede:

- Utilização da Largura de Banda da Rede: Utilização média da largura de banda em todas as NICs.

- Contagem de Reconexões do Servidor: Número de vezes que o servidor se reconectou devido a problemas de rede ou rebalanceamento do servidor ou desligamentos e reinícios do Serviço de Stream do Citrix Provisioning™.
- Contagem Total de Tentativas de UDP: Número de vezes que o dispositivo de destino de provisionamento tentou se reconectar ao servidor de provisionamento usando UDP. Essa métrica ajuda você a saber se há algum problema de rede no Serviço de Stream do Citrix Provisioning (por exemplo, configurações de switch incorretas).

Inicialização:

- MB de Bytes Lidos na Inicialização: Bytes lidos durante a inicialização.
- MB de Bytes Gravados na Inicialização: Bytes gravados durante a inicialização.
- Inicializar De: Meio de inicialização (vDisk, disco local e assim por diante).
- Contagem de Tentativas de Inicialização: Número de tentativas de inicialização da máquina.
- Tempo de Inicialização: Tempo levado para inicializar a máquina, em segundos. Por padrão, há um atraso de 5 segundos entre as tentativas. Se esse atraso aumentar para dois dígitos, haverá um aumento significativo no tempo de inicialização. Verifique sua configuração de provisionamento para resolver esse problema.
- Versão do Software de Destino: Versão do software do dispositivo de destino de Provisionamento.
- Nome do vDisk: vDisk do qual o dispositivo de destino de Provisionamento está inicializando.

Cache:

- Tipo de Cache de Gravação: o vDisk pode ser configurado para diferentes tipos de cache. Para obter mais informações, consulte o artigo da Central de Conhecimento CTX119469.
- Letra da Unidade do Volume de Cache de Gravação: Letra da unidade para tipos de cache de gravação que envolvem unidades.
- Tamanho do Volume de Cache de Gravação MB: Tamanho total do volume configurado para cache de gravação.
- Tamanho do Arquivo de Cache MB: Tamanho atual do arquivo de cache (cache na RAM do dispositivo com estouro no disco rígido).
- Uso de Cache RAM MB: Tamanho atual do cache RAM (cache na RAM do dispositivo com estouro no disco rígido). Use o estouro para disco somente se necessário. Essa métrica é útil ao definir ou otimizar o tamanho adequado do cache RAM.

Para obter mais informações, consulte Usando a Bandeja de Status em um dispositivo de destino.

As métricas do dispositivo de destino do Provisioning estão disponíveis apenas em:

- Máquinas do Provisioning.
- Versão 7.19 e posterior do dispositivo de destino do Provisioning.
- Versão 2003 e posterior do VDA.

> **Nota:**
>
> As métricas para Contagem de Reconexões do Servidor e Contagem de Tentativas UDP estão disponíveis apenas para a versão 1912 CU2 e posterior do destino do Provisioning.

Monitoramento de infraestrutura

O Citrix Monitor agora oferece visibilidade sobre a saúde operacional dos componentes do Citrix DaaS™. Este recurso ajuda você a identificar, solucionar e resolver facilmente problemas relacionados à sua infraestrutura. Atualmente, a saúde dos seguintes componentes é monitorada:

- Cloud Connector
- Serviço Citrix Provisioning™
- StoreFront™
- Connector Appliance

Para oferecer suporte a este recurso, um novo executável do Windows chamado `citrixinframonitor.msi` foi introduzido para os componentes Citrix. Isso auxilia na coleta e transmissão de métricas de saúde relevantes dos servidores Provisioning Service ou StoreFront para o Monitor. No entanto, `citrixinframonitor.msi` não é necessário para monitorar o Cloud Connector. Os Cloud Connectors são automaticamente integrados quando uma conexão entre o Citrix Cloud e seus locais de recursos é estabelecida.

Este recurso ajuda você a obter conjuntos de dados de monitoramento críticos e alertas proativos sobre as métricas de sistema do Cloud Connector, Provisioning Service e servidor StoreFront em um único console no Monitor. Os dados são coletados a cada cinco minutos dos componentes de monitoramento para garantir as informações mais recentes.

Este recurso visa aprimorar a eficiência operacional, oferecendo monitoramento proativo, métricas detalhadas e alertas automatizados, garantindo que sua infraestrutura Citrix funcione de forma suave e eficiente.

Principais recursos

Monitoramento em tempo real:

- Monitoramento contínuo dos componentes da infraestrutura Citrix, como Cloud Connector, servidores Citrix Provisioning (Provisioning Service), StoreFront e Connector Appliance.
- Visualizações de painel apresentando a saúde do sistema, utilização de recursos e métricas de desempenho relevantes.

Análise detalhada:

- Fornece análise detalhada sobre as métricas de saúde do sistema, como status de conectividade e status de serviço ou processo para cada componente.
- Detalhes sobre as métricas de utilização de recursos, como CPU, memória e utilização de disco.

Alertas e notificações automatizados:

- Limites de alerta personalizáveis para várias métricas e estados com escopos granulares.
- Notificações em tempo real por e-mail e webhooks.

Casos de uso

Eficiência operacional:

Garante que as equipes de administração da Citrix possam manter alta disponibilidade e desempenho de seus servidores e serviços Citrix. Esse recurso também ajuda a minimizar o tempo de inatividade, identificando proativamente e alertando os administradores sobre problemas antes que eles afetem grupos de usuários significativos.

Resolução mais rápida de tickets:

Monitora as principais métricas de integridade e desempenho do servidor para avaliar a entrega ideal de aplicativos e desktops virtuais aos usuários. Use essas métricas para diagnosticar e resolver reclamações de usuários relacionadas ao desempenho, analisando os componentes associados.

Pré-requisitos

- Certifique-se de que os pré-requisitos para o Provisioning Service ou os pré-requisitos para o StoreFront sejam atendidos.
- Para monitorar o Citrix Provisioning:

    - Versão mínima necessária para monitorar a Conectividade do Banco de Dados e a Acessibilidade do Servidor de Licenças:
        - 2402 CU1
        - 2407
    - A versão mínima necessária para monitorar o Serviço PXE, o Serviço TFTP e a Contagem Total de Reconexões é o Citrix Infra Monitor 2411.

- Contas de usuário ou permissões necessárias para executar o Citrix Infrastructure Monitor:
    - Contas de usuário com permissões de administrador do Windows para instalar o Citrix Infrastructure Monitor nas máquinas de endpoint.
    - Uma conta de usuário de administrador completo ou uma função personalizada com as seguintes permissões de Monitoramento:
        - Criar\Editar\Habilitar\Excluir Políticas de Alerta
        - Criar\Editar\Remover Configuração do Servidor de E-mail de Alerta
        - Descartar Alertas
        - Visualizar Políticas de Alerta
        - Visualizar Alertas
        - Visualizar página do Painel
        - Visualizar página do Monitor de Infraestrutura
        - Para visualizar a página de **Alertas**

> **Nota:**
>
> - O pré-requisito anterior é válido apenas para o monitoramento dos componentes do Provisioning Service e do StoreFront.
> - Se você não tiver permissão para acessar a página de **Alertas**, a opção **Gerenciar Alertas** será desabilitada na página de **Monitoramento de Infraestrutura**.

Para começar a usar e implementar o recurso **Monitoramento de Infraestrutura** em seu site, consulte o seguinte:

- Introdução ao Monitoramento de Infraestrutura

- Configurar SDK do PowerShell Remoto
- Gerenciar conexões
- Painel de infraestrutura
- Políticas de alerta avançadas
- Políticas de infraestrutura

Introdução ao Monitoramento de Infraestrutura

> **Nota:**
>
> Os dois passos a seguir são válidos apenas para o monitoramento de componentes do Provisioning Service e StoreFront™.

Etapa 1: Instalação do Citrix Infrastructure Monitor

Execute os passos a seguir para concluir a instalação no componente de destino e estabelecer a conexão para coleta segura de dados.

Etapa 1.1: Identificar os componentes de destino

Identifique os componentes de destino, como servidores Provisioning Service ou StoreFront, que precisam ser monitorados.

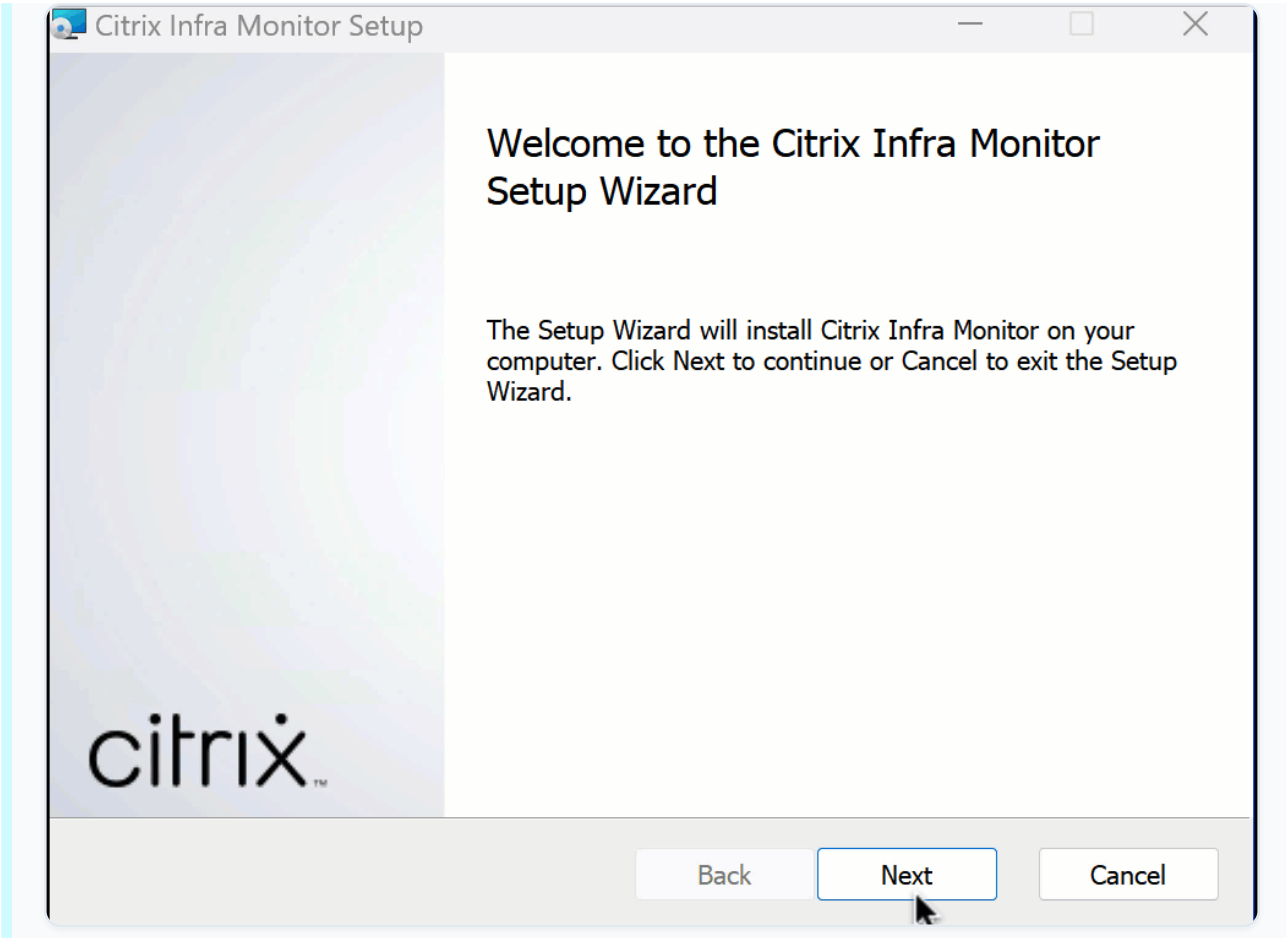
Etapa 1.2 Baixar o Citrix Infrastructure Monitor

Você pode baixar `CitrixInfraMonitor.msi` na página downloads da Citrix no servidor de destino identificado na Etapa 1.1.

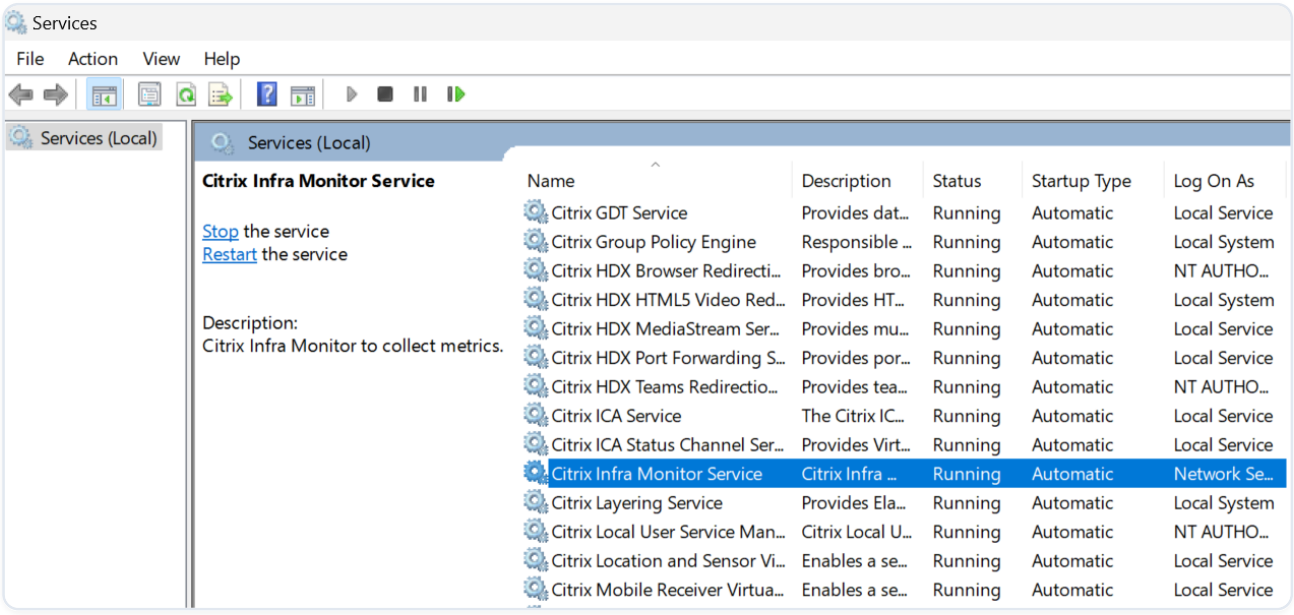
Etapa 1.3: Executar o Citrix Infrastructure Monitor

Execute o instalador `CitrixInfraMonitor.msi` no componente de destino seguindo as instruções do assistente de instalação.

> **Nota:**
>
> Usuários com privilégios administrativos podem instalar e configurar o Citrix Infrastructure Monitor no componente de destino.



Após a instalação ser bem-sucedida, você pode visualizar o Serviço de Monitoramento de Infraestrutura Citrix na seção **Serviços**:



Etapa 1.4: Obtenha o token de registro

Obtenha o token fornecido no arquivo `RegistrationToken.txt` em `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` no sistema onde o Monitor de

Infraestrutura Citrix está instalado e mantenha-o pronto para uso em Etapa 2: Registrar o Monitor de Infraestrutura Citrix.

REQUISITOS DE PORTA

Após instalar `CitrixInfraMonitor.msi` com sucesso, o instalador cria uma exceção para a porta 9595. Se você estiver usando um firewall de terceiros, talvez precise permitir manualmente a comunicação TCP para esta porta para usar o serviço de Monitoramento de Infraestrutura Citrix.

A tabela a seguir fornece detalhes sobre os requisitos de porta de entrada para máquinas do Provisioning Service e StoreFront:

ORIGEM	DESTINO	TIPO	PORTA	PROTOCOLO	FINALIDADE
Cloud Connector	Máquina do Provisioning Service ou StoreFront	TCP	9595	HTTP ou HTTPS	Chamada para coletar métricas do Serviço de Provisionamento ou da máquina StoreFront.

> **Nota:**
>
> As máquinas do Serviço de Provisionamento e do StoreFront não fazem chamadas de saída para o serviço de Monitoramento de Infraestrutura.

Etapa 2: Registrar o Citrix Infrastructure Monitor

Você pode registrar o Citrix Infrastructure Monitor usando o seguinte:

- Interface do usuário do Monitor
- SDK do PowerShell Remoto

Usando a Interface do usuário do Monitor

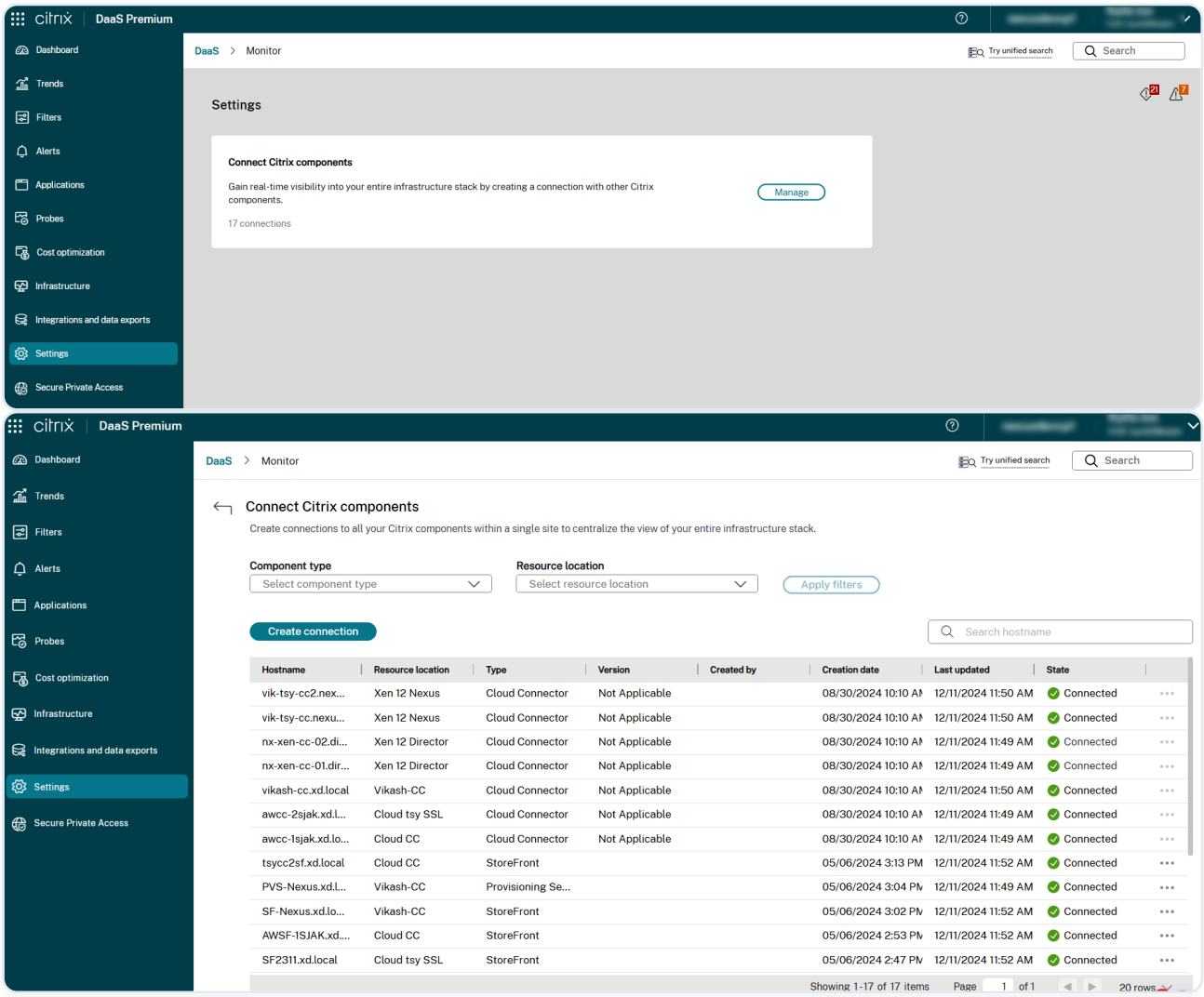
Conclua o registro na Interface do usuário do Monitor executando as seguintes etapas.

ETAPA 2.1: NAVEGAR PARA A PÁGINA CONECTAR COMPONENTES CITRIX

Clique em **Configurações** > **Conectar componentes Citrix** > **Gerenciar**.

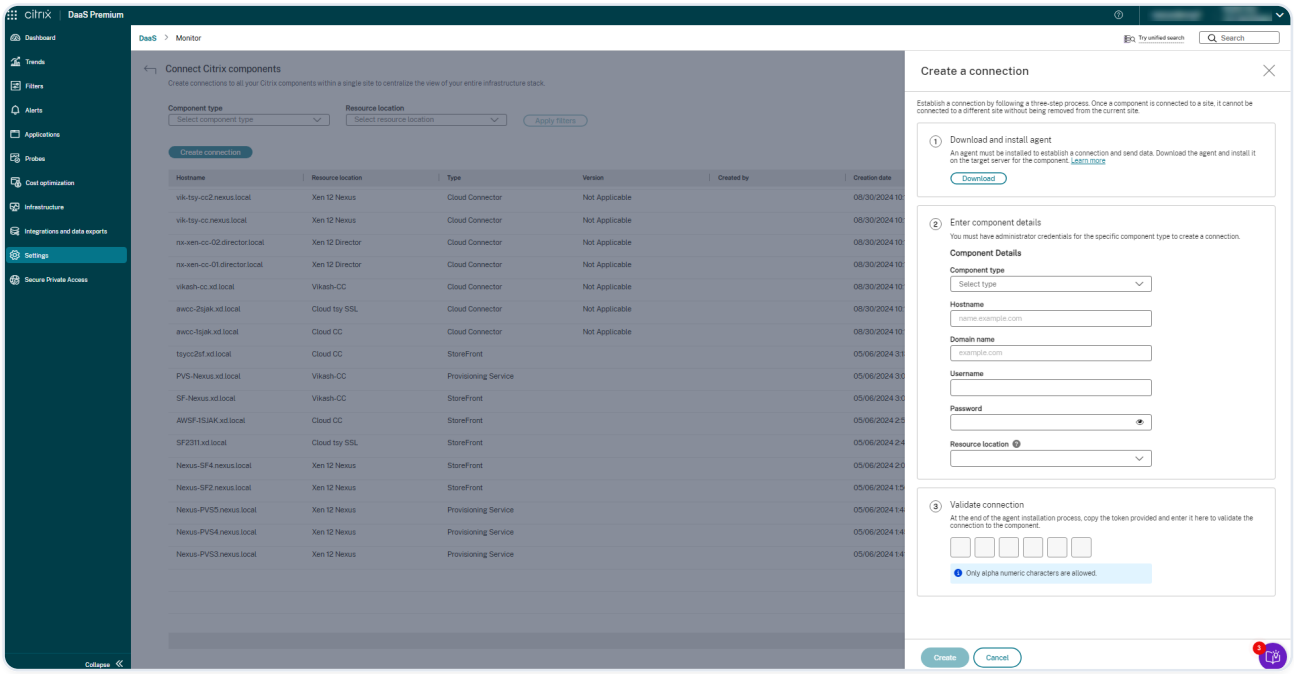
Ou,

Clique em **Infraestrutura** > **Gerenciar**.



ETAPA 2.2: INSERIR DETALHES DO COMPONENTE

Na tela **Conectar componentes Citrix**, clique em **Criar conexão**. A janela **Criar uma conexão** é exibida.



Certifique-se de que o `citrixinframonitor.msi` seja baixado e instalado no destino. Para obter mais informações, consulte Etapa 1 neste documento. Siga as instruções na tela e preencha os detalhes do componente necessários para estabelecer uma conexão segura.

- Selecione um **Tipo de componente** na lista suspensa. Pode ser Provisioning Service ou StoreFront.
- Insira o **Nome do host**.
- Insira o **Nome de domínio**.
- Insira o **Nome de usuário** da máquina Provisioning Service ou StoreFront.
- Insira a **Senha** da máquina Provisioning Service ou StoreFront.
- Selecione o **Local do recurso**.

ETAPA 2.3: AUTORIZAR A CONEXÃO

Obtenha o token do Citrix Infrastructure Monitor do arquivo `RegistrationToken.txt` em `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` no sistema onde o Citrix Infrastructure Monitor está instalado.

Insira os detalhes do token obtido na interface do usuário do Director. Isso autoriza a conexão entre o site e o componente.

O texto do token presente no arquivo `RegistrationToken.txt` é regenerado quando você reinicia o serviço Citrix Infrastructure Monitor. Após o registro ser bem-sucedido, o arquivo de token é excluído da máquina. Se você precisar recriar um novo arquivo de token por qualquer motivo, reinicie o serviço Citrix Infrastructure Monitor. Por motivos de segurança, o arquivo de token é removido após três tentativas de registro falhas com um token inválido.

ETAPA 2.4: CRIAR CONEXÃO

Depois que os detalhes forem preenchidos, clique em **Criar**. A conexão criada estará disponível na lista de conexões na página **Conectar componentes Citrix**.

Usando o SDK do PowerShell Remoto

> **Nota:**
>
> A versão mínima exigida do PoshSDK é 7.42.26154.48609 ou posterior.

1. Certifique-se de que os pré-requisitos mencionados em Pré-requisitos sejam atendidos.
2. Configurar o SDK do PowerShell Remoto.
3. Execute o seguinte comando PowerShell para registrar o Citrix Infrastructure Monitor:

```
Add-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component> -AdminAddress localhost:19097 -ResourceLocationId
<resourceLocationID> -Domain <domain> -Username <username> -Password
<password> -Token <token>
```

> **Nota:**
>
> O nome de usuário e a senha são parâmetros opcionais. No entanto, se você não fornecer esses parâmetros, algumas das métricas não estarão disponíveis para você.

> Os parâmetros do comando anterior são os seguintes:

PARÂMETRO	DESCRIÇÃO
`Fqdn`	FQDN do Serviço de Provisionamento ou servidor StoreFront.
`Component`	O componente que você está integrando. Por exemplo: Serviço de Provisionamento ou SF. Serviço de Provisionamento significa Citrix Provisioning™ e SF significa StoreFront.

PARÂMETRO	DESCRIÇÃO
`ResourceLocationId`	O ID do local do recurso do site. Para recuperar esse valor, selecione o botão **ID** localizado abaixo do nome do local do recurso na página **Locais de Recursos** no Citrix Cloud.
`Domain`	O domínio do qual todos os componentes fazem parte.
`Username`	Nome de usuário do administrador.
`Password`	Senha do usuário administrador.
`Token`	Obtenha o token do Citrix Infrastructure Monitor do arquivo `RegistrationToken.txt` em `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` no sistema onde o Citrix Infrastructure Monitor está instalado.

Nota:

- O texto do token presente no arquivo `RegistrationToken.txt` é regenerado quando você reinicia o serviço Citrix Infrastructure Monitor. Após o registro ser bem-sucedido, o arquivo de token é excluído da máquina. Se você precisar registrar novamente, reinicie o serviço Citrix Infrastructure Monitor.
- Por motivos de segurança, o arquivo de token é removido após três tentativas de registro falhas com um token inválido.

Depois de registrar com sucesso a máquina do Provisioning Service ou StoreFront, os detalhes do nome da máquina aparecem na guia **Monitor** > **Infraestrutura**.

Um exemplo de comando para se registrar no Citrix Infrastructure Monitor é o seguinte:

```
Add-MonitorDirectorAgent -Component PVS -Fqdn [redacted]
-ResourceLocationId [redacted] -Domain xd.local
-Username administrator -Password "[redacted]" -AdminAddress
localhost:19097 -Token [redacted]
```

Etapas para configurar HTTPS para o Citrix Infrastructure Monitor

> **Nota:**
>
> O serviço Citrix Infrastructure Monitor também funciona no modo HTTP e, neste caso, a seguinte configuração não é necessária. No entanto, recomendamos que você o use no modo HTTPS. **Execute as seguintes etapas somente se precisar configurar HTTPS para o Citrix Infrastructure Monitor**.

Etapa 1: Carregar o certificado para a máquina

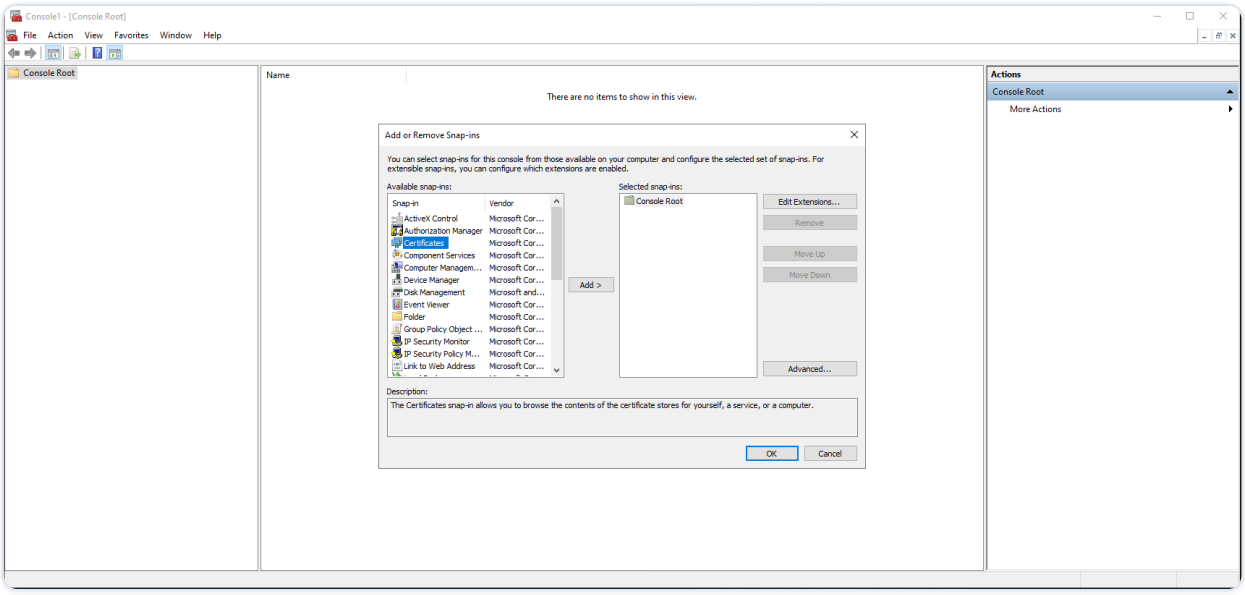
1. Obtenha um certificado PFX para sua máquina onde o Citrix Infrastructure Monitor está instalado. Para obter mais informações sobre a geração de arquivos PFX, consulte Como criar um arquivo PFX.

   > **Nota:**
   >
   > Você também pode usar arquivos PFX protegidos por senha.

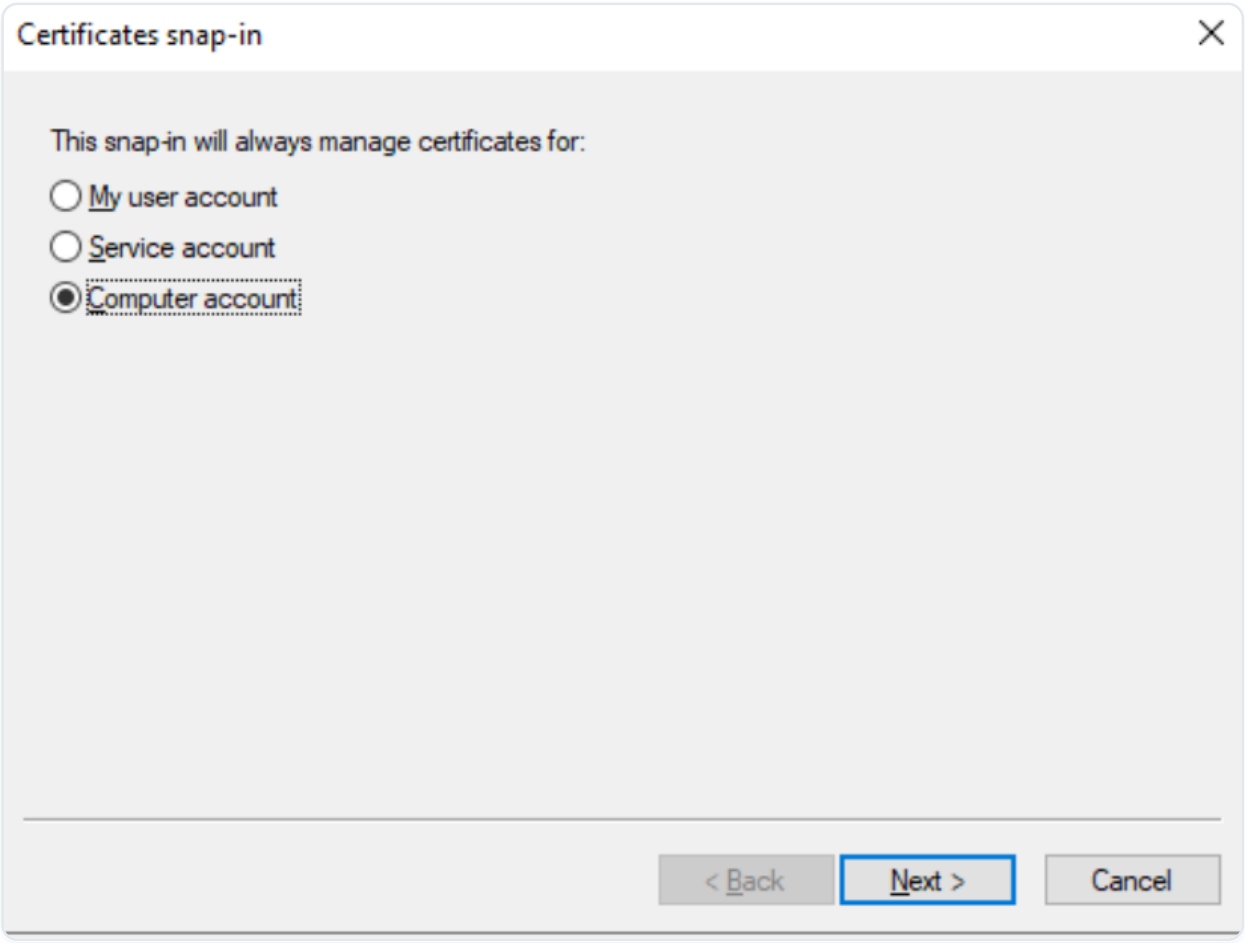
2. Carregue o certificado para a máquina em qualquer local.

Etapa 2: Importar o certificado para os certificados do computador

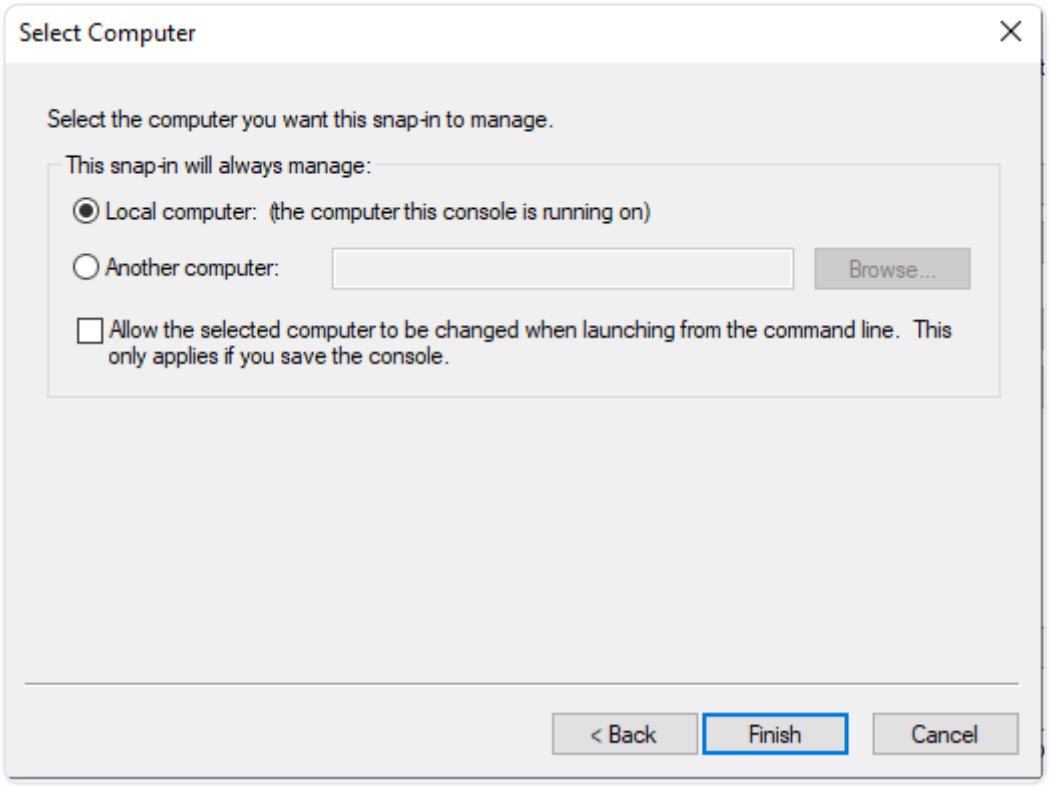
1. Clique em **Iniciar** > **Executar** > digite `mmc` e, em seguida, clique em **OK**. A janela **Console 1 -** é exibida.
2. No menu **Arquivo**, clique em **Adicionar/Remover Snap-in**. A janela **Adicionar ou Remover Snap-ins** é exibida.



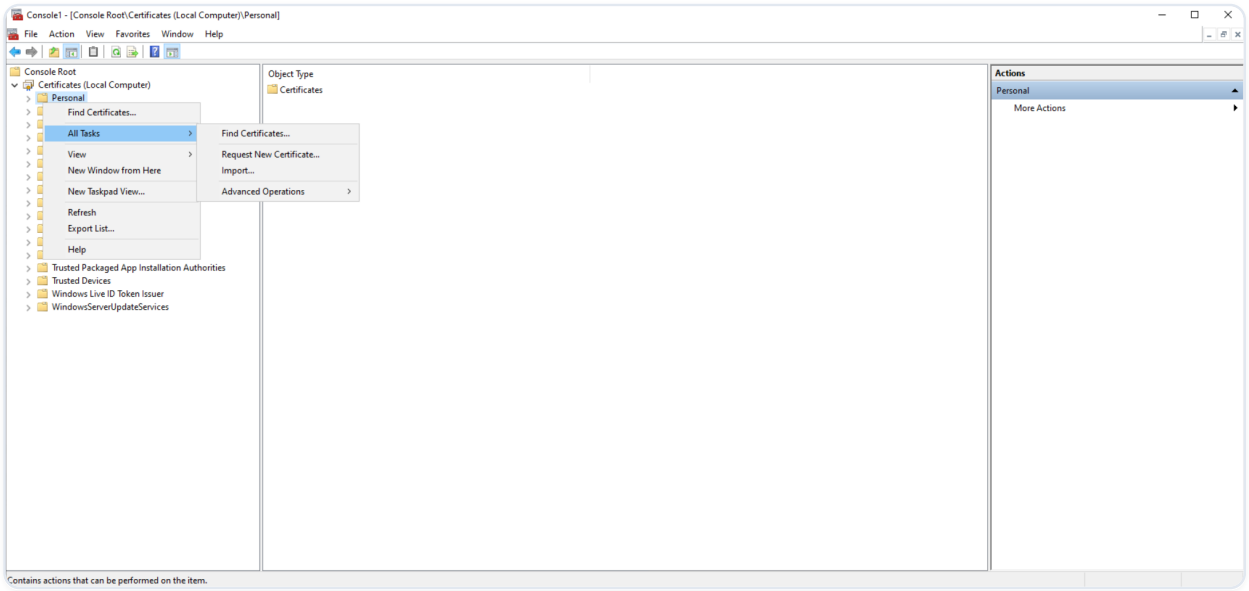
3. Em **Snap-in**, clique duas vezes em **Certificados**. A janela **Snap-in de Certificados** é exibida.



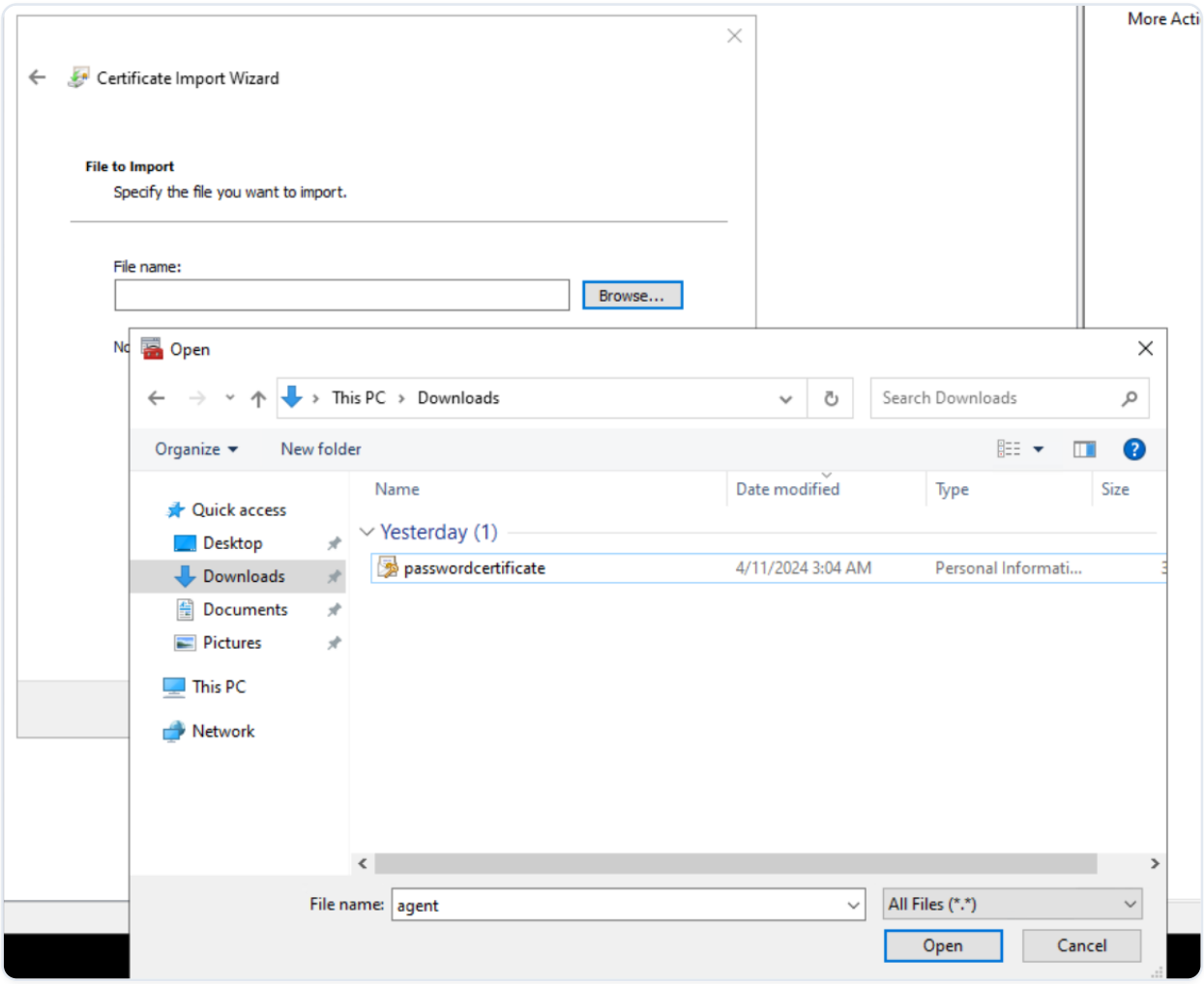
4. Selecione **Conta de computador** e clique em **Avançar**. A janela **Selecionar Computador** é exibida.



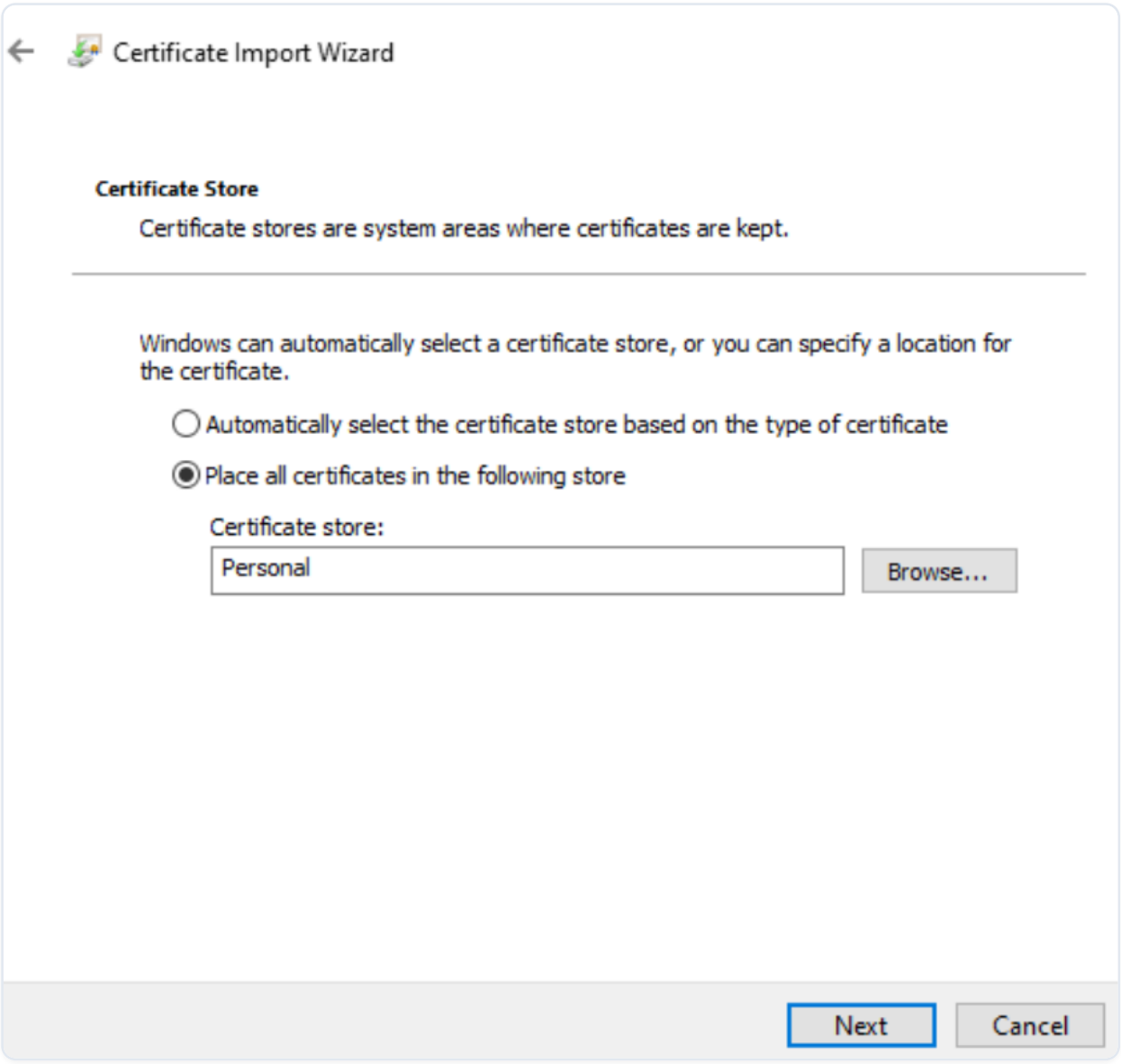
5. Selecione **Computador local**.
6. Clique em **Concluir**. A seção **Certificados (Computador Local)** aparece na lista de snap-ins selecionados para o novo console.
7. Clique em **OK**.
8. Expanda **Certificados**, clique com o botão direito em **Pessoal** > **Todas as Tarefas** > **Importar**. O **Assistente para Importação de Certificados** é exibido.



9. Selecione **Avançar** > **Procurar Arquivos**. navegar até o local onde você carregou o arquivo PFX, altere o tipo de arquivo para **Todos os arquivos** e, em seguida, selecione o certificado PFX respectivo.



10. Insira a senha PFX. Você pode deixá-lo em branco se não houver senha.
11. Clique em **Avançar**.
12. Para o Repositório de Certificados, certifique-se de que a opção **Colocar todos os certificados no seguinte repositório** esteja selecionada e que o **Repositório de certificados** esteja selecionado como **Pessoal**.



13. Clique em **Avançar**.
14. Revise os detalhes e clique em **Concluir**.
15. Aguarde a confirmação. A mensagem *A importação foi bem-sucedida* é exibida.
16. navegar para **Certificados** > **Pessoal** e certifique-se de que o certificado esteja presente.
17. Exclua o arquivo de certificado PFX da máquina.

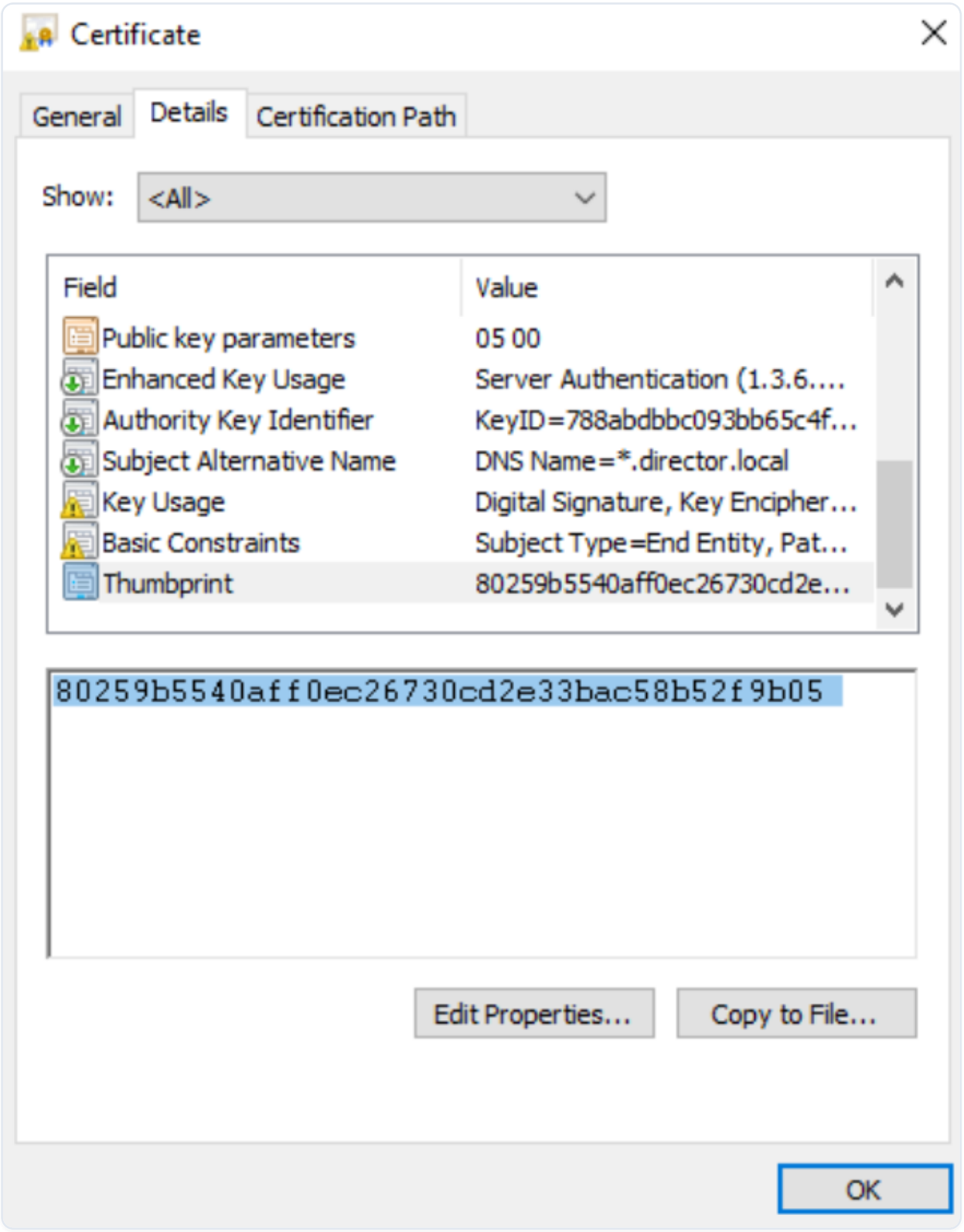
Etapa 3: Fornecer acesso de leitura ao certificado

1. Clique com o botão direito do mouse no certificado importado > **Todas as Tarefas** > **Gerenciar Chaves Privadas**.
2. Na caixa de diálogo que se abre, selecione **Adicionar** e, em seguida, procure por **Serviço de Rede**. Clique em **OK**.
3. Selecione **NETWORK SERVICE** em **Grupo** ou **nomes de usuário**.

4. Permita o acesso de *Leitura* em **Permissões para NETWORK SERVICE**.
5. Clique em **OK**.

Etapa 4: Obter o Thumbprint

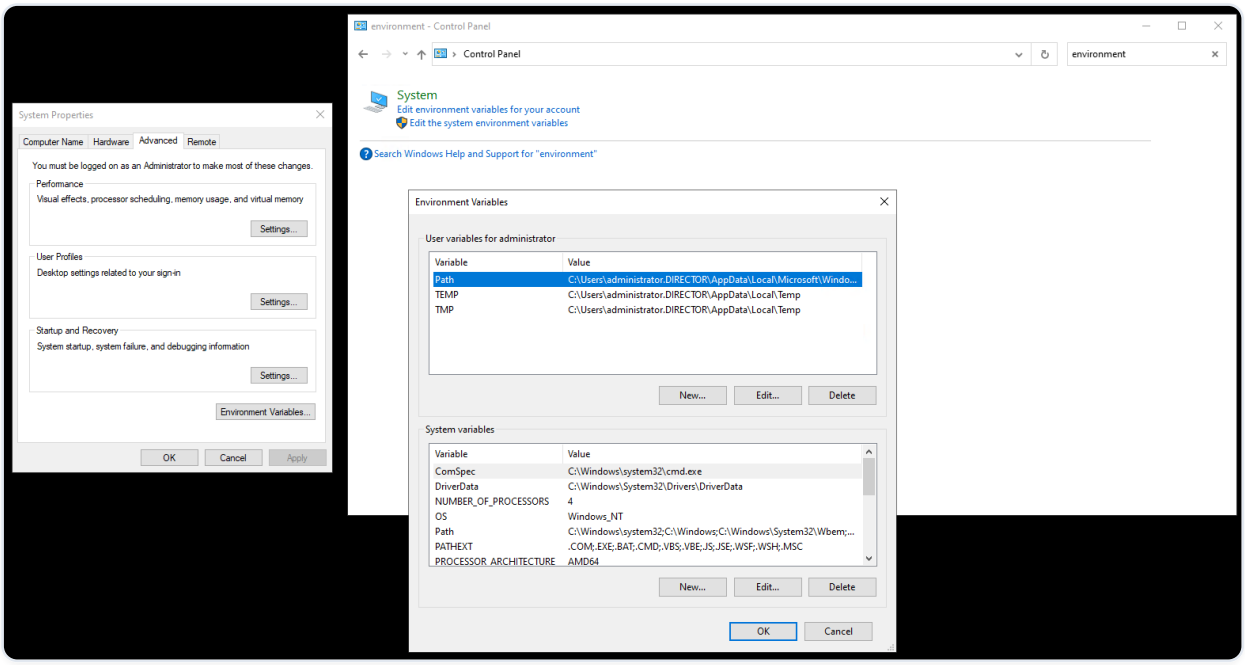
1. Clique duas vezes no certificado importado.
2. Na caixa de diálogo que se abre, navegar para a guia **Detalhes** e role até o final.
3. Clique em **Impressão digital**.



4. Copie o valor e o mantenha pronto para a próxima etapa.

Etapa 5: Definindo a variável de ambiente

1. Abra o Painel de Controle.
2. Pesquise por ambiente e selecione **Editar as variáveis de ambiente do sistema**.
3. Em **Variáveis do Sistema (para todos os usuários)**, clique em **Novo**.



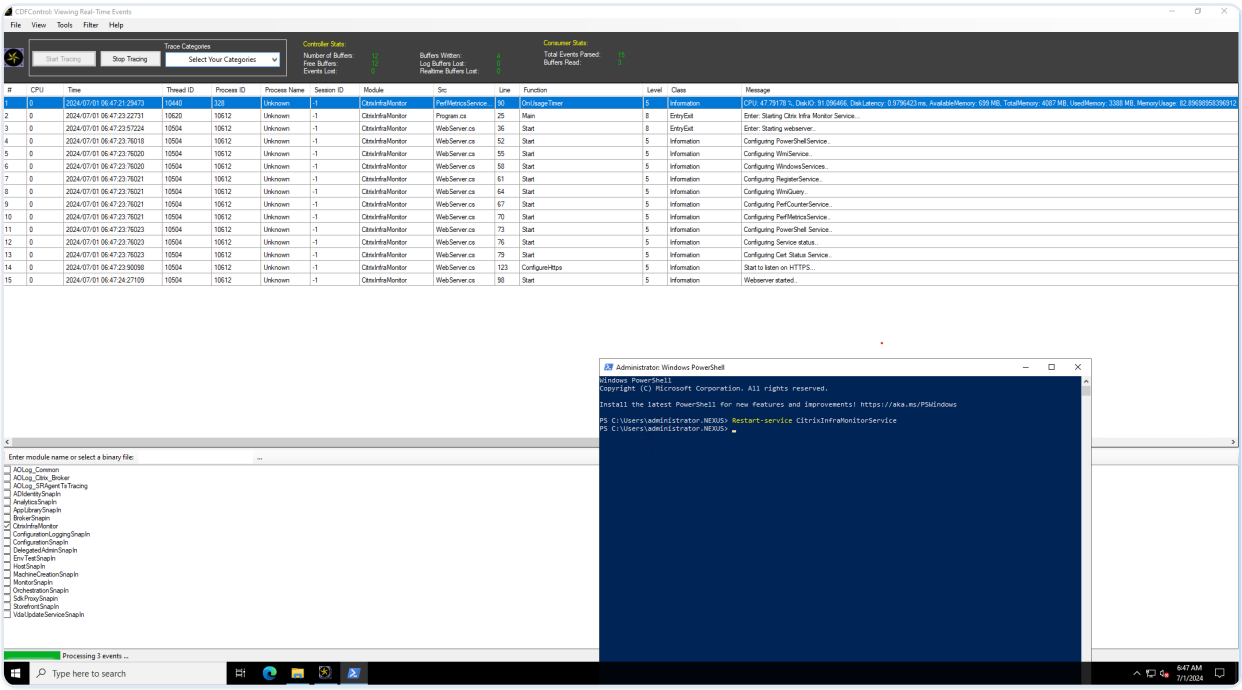
4. Especifique o nome da **Variável** como *DIRECTOR_AGENT_HTTPS_CERTIFICATE_THUMBPRINT*.
5. Especifique a impressão digital da etapa anterior em valor da **Variável**.
6. Clique em **OK**.

Etapa 6: Reiniciar CitrixInfraMonitorService

1. Abra o PowerShell e execute o seguinte comando:

```
Restart-Service CitrixInfraMonitorService
```

2. Certifique-se de que o HTTPS esteja habilitado capturando o módulo **CitrixInfraMonitorService** e procurando pela linha de log **Start to listen on HTTPS...**.



Passo 7: Habilitar HTTPS na configuração do Monitor

Você pode habilitar HTTPS no serviço Monitor, usando o SDK do PowerShell Remoto.

> **Nota:**
>
> A versão mínima exigida do PoshSDK é 7.44.26401.2361 ou posterior.

1. Certifique-se de que os pré-requisitos mencionados em Pré-requisitos sejam atendidos.
2. Configurar o SDK do PowerShell Remoto.
3. Execute o seguinte comando PowerShell para habilitar HTTPS na configuração do Monitor:

```
Set-DirectorAgentHttps -AdminAddress localhost:19097 -EnableHttps $true
```

> **Nota:**
>
> Para verificar o valor das configurações existentes, execute o comando `Get-DirectorAgentHttps -AdminAddress localhost:19097`.

> Caso precise desabilitar HTTPS na configuração do Monitor, execute o comando `Set-DirectorAgentHttps -AdminAddress localhost:19097 -EnableHttps $false`.

Configurar o SDK Remoto do PowerShell

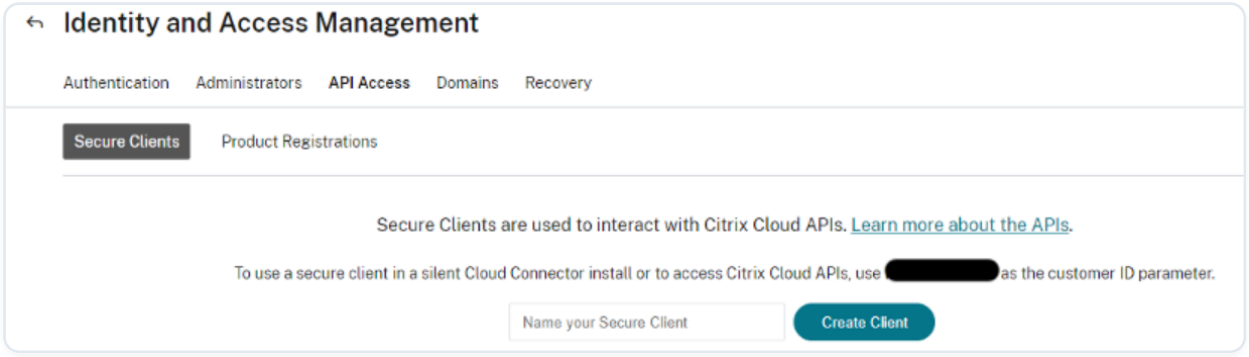
Pré-requisitos

- Certifique-se de que o Citrix Infrastructure Monitor esteja instalado na máquina StoreFront™ ou Provisioning Service.
- Você deve primeiro instalar o SDK Remoto do PowerShell em qualquer máquina ingressada no domínio dentro do mesmo local de recurso. Para obter mais informações, consulte a documentação SDK e API.

Configuração do SDK Remoto do PowerShell

Execute as seguintes etapas e os comandos do PowerShell no dispositivo onde você instalou o SDK Remoto do PowerShell:

1. Faça login no console do Citrix Cloud™ com suas credenciais do Citrix Cloud.
2. navegar para **Identity and Access Management**.
3. Vá para a guia **API access** > **Secure Clients** > **Name your Secure Client** e clique em **Create Client**.



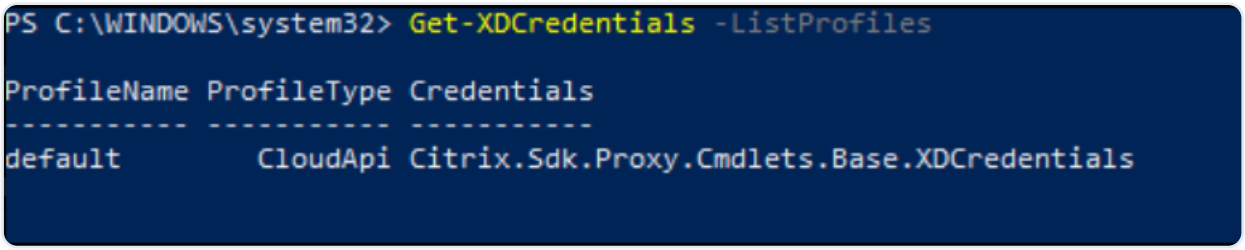
4. Depois de criar o cliente, o ID e o segredo podem ser baixados em um arquivo CSV para uso futuro.
5. Para configurar a conexão com o ambiente Citrix Cloud, use o Segredo do Cliente criado na etapa anterior. O comando de exemplo a ser usado no PowerShell é o seguinte:

```
Set-XDCredentials -CustomerId “<customerid>” -SecureClientFile “c:
\temp\secureclient.csv” -ProfileType CloudAPI –StoreAs “default”
```

6. Liste os perfis do PowerShell Citrix Cloud armazenados localmente no computador usando os seguintes comandos do PowerShell:

```
Get-XDCredentials -ListProfiles
```

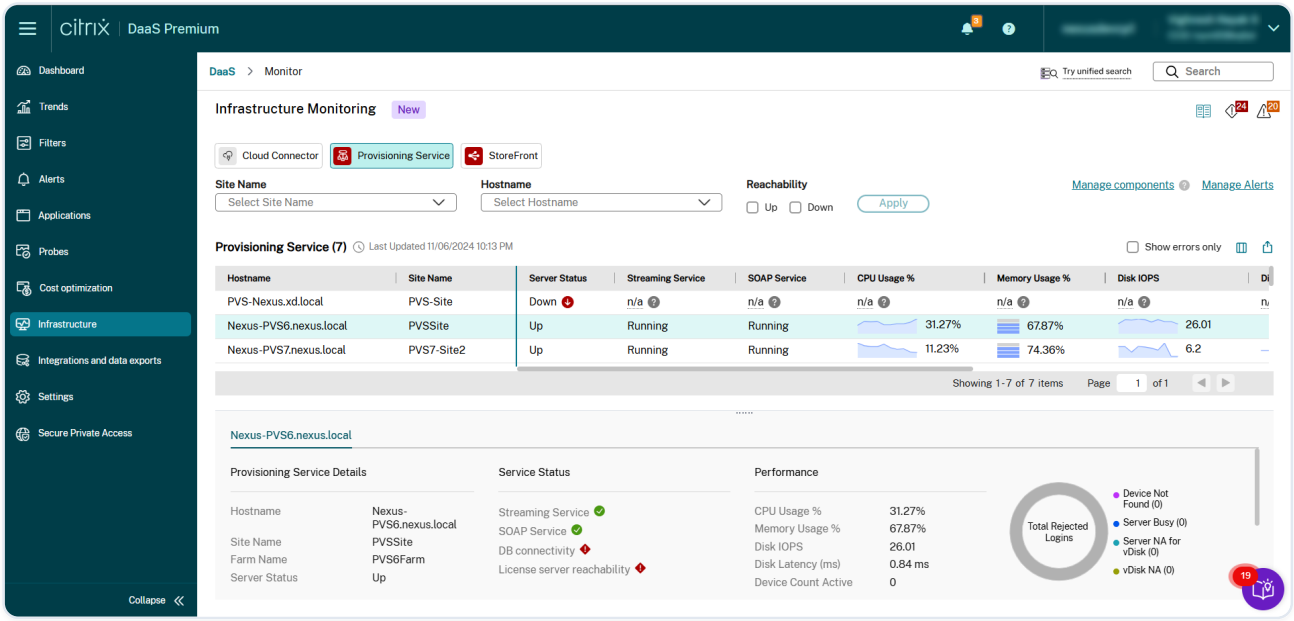
A imagem a seguir mostra os comandos anteriores conforme inseridos no PowerShell:



Para obter mais informações, consulte SDK PowerShell Remoto do Citrix DaaS.

Gerenciar conexões

Você pode visualizar, remover ou editar as conexões na página **Conectar componentes Citrix®**.



Visualizar conexões

Você pode visualizar os detalhes de todos os componentes conectados e desconectados disponíveis nesta visualização. A tabela a seguir descreve as diferentes colunas da página **Criar conexão**:

COLUNA	DESCRIÇÃO
Nome do host	O FQDN do servidor.
Localização do recurso	A localização do recurso configurada para alcançar o componente.

COLUNA	DESCRIÇÃO
Tipo	O tipo de conexão. Pode ser Provisioning Service e StoreFront.
Versão	A versão do `CitrixInfraMonitor.msi` instalada no componente.
Criado por	O nome do administrador que criou a conexão.
Data de criação	A data em que a conexão é estabelecida.
Última atualização	A data em que a conexão foi atualizada pela última vez.
Estado	Os diferentes estados são Conectando, Conectado e Desconectado.
	• **Conectando**: Este estado indica que pode levar aproximadamente cinco minutos para que os dados apareçam para o novo componente e aproximadamente 10 minutos para que os dados de utilização de recursos estejam disponíveis.
	• **Conectado**: Este estado indica que a conexão entre os componentes e o site está ativa e funcionando.
	• **Desconectado**: Este estado indica que a conexão entre os componentes e o site está desconectada. As possíveis razões para o estado Desconectado incluem tempo de inatividade do servidor ou o site não conseguir se conectar ao Citrix Infrastructure Monitor.

> **Nota:**
>
> As conexões do Cloud Connector são preenchidas automaticamente nesta visualização quando conectadas ao site da nuvem.

Editar a conexão

A edição da conexão pode ser necessária para atualizar as credenciais de administrador usadas para estabelecer o Provisioning Service ou a conexão do StoreFront.

Para editar uma conexão existente, faça o seguinte:

1. navegar para a página **Conectar componentes Citrix** na guia **Configurações** ou **Infraestrutura**.
2. Na tabela da lista de conexões, clique nos três pontos no final da linha do componente de interesse.
3. Clique em **Editar** e atualize os detalhes conforme necessário.

Remover um componente

Você pode fazer isso na interface do usuário do Monitor ou usando o comando PowerShell.

Usando a interface do usuário do Monitor

Remover um componente é um processo de cancelamento de registro de um serviço de provisionamento ou conexão StoreFront do Monitor. Uma vez concluído o processo de cancelamento de registro, a coleta de novos dados é interrompida para o componente selecionado. Para remover uma conexão existente:

1. navegar para a página **Conectar componentes Citrix** na guia **Configurações** ou **Infraestrutura**.
2. Na tabela da lista de conexões, clique nos três pontos no final da linha do componente de interesse.
3. Clique em **Remover**. A conexão é cancelada e removida do Monitor.

Usando o comando PowerShell

Caso precise cancelar o registro de um determinado componente, execute o seguinte comando PowerShell no dispositivo onde o PoshSDK está instalado:

```
Remove-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component> -ResourceLocationId <resourceLocationID> -AdminAddress
localhost:19097
```

Um exemplo de comando para remover o registro do Citrix Infrastructure Monitor é o seguinte:

```
Remove-MonitorDirectorAgent -Component SF -Fqdn [redacted]
-ResourceLocationId [redacted] -AdminAddress
localhost:19097
```

Nota:

Desregistrar um componente apenas interrompe o fluxo de dados do componente específico para o Monitor. Se você precisar desinstalar o Citrix Infrastructure Monitor, desinstale-o do Painel de Controle.

Painel de infraestrutura

Você pode ver os valores de integridade dos seus componentes na página **Monitoramento de Infraestrutura**. Esses resultados ajudam a analisar e solucionar problemas proativamente relacionados à sua infraestrutura.

Você pode filtrar a página **Monitoramento de Infraestrutura** por:

- Nome do host - Selecione o nome do host
- Acessibilidade - Selecione a caixa de seleção **Ativo** (servidor acessível) ou **Inativo** (servidor não acessível)
- Erros - Selecione a caixa de seleção Mostrar linhas com erros apenas.

Use a opção **Gerenciar colunas** para escolher os dados a serem exibidos no seu painel.

Métricas de integridade do Provisioning Service

Clique na guia **Infraestrutura** e selecione **Provisioning Service**. O painel de infraestrutura para Provisioning Service aparece:

Painel do Provisioning Service(/en-us/citrix-daas/media/sm-pvs-dashboard.png)

Os seguintes detalhes são monitorados para os servidores do Provisioning Service:

CATEGORIA	MÉTRICAS	DESCRIÇÃO
Acessibilidade	Nome do host	O nome da máquina do Provisioning Service onde o Citrix Infrastructure Monitor está instalado. Esta métrica é um valor de string.
	Nome do Site do Provisioning Service	O nome do site do Provisioning Service. Esta métrica é um valor de string.
	Nome da Farm do Provisioning Service	O nome da farm do Provisioning Service. Esta métrica é um valor de string.
	ID do Site do Provisioning Service	Exibe o ID do site do servidor do Provisioning Service. Esta métrica é um valor de string.
	ID da Farm do Provisioning Service	Exibe o ID da farm do servidor do Provisioning Service. Esta métrica é um valor de string.
	Status do Servidor	Mostra o estado de acessibilidade do servidor fornecido. Os valores possíveis são *Up*, *Down* e *Unknown*.
	Última Inicialização	Exibe a hora em que o servidor do Provisioning Service foi inicializado pela última vez.
	Última atualização	Exibe a hora em que os dados foram coletados do servidor do Provisioning Service.

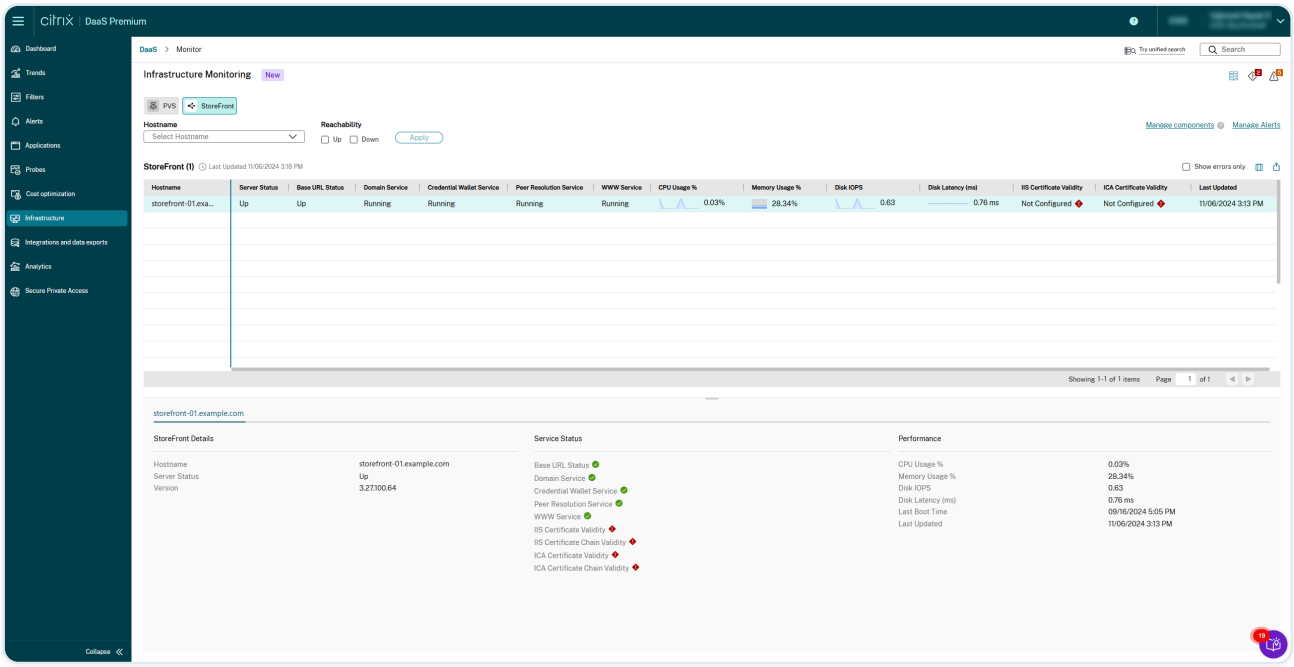
CATEGORIA	MÉTRICAS	DESCRIÇÃO
Serviços Dependentes	Serviço de Streaming	Exibe o status do serviço de streaming. Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: *Not running*, *Running*, *Not Installed* e *n/a* (com ícone de ajuda).
	Serviço SOAP	Exibe o status do serviço Simple Object Access Protocol (SOAP). Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: *Not running*, *Running*, *Not Installed* e *n/a* (com ícone de ajuda).
	Conectividade do BD	Exibe o status da conectividade do banco de dados. Se você estiver usando um servidor Citrix Provisioning versão 2402 ou anterior, poderá receber um erro desconhecido. Os valores possíveis são *Não Conectado*, *Conectado*, *Desconhecido* e *n/a* (com ícone de ajuda).
	Acessibilidade do Servidor de Licenças	Exibe se o servidor de licenças está acessível ou não. Se você estiver usando o servidor Citrix Provisioning versão 2402 ou anterior, poderá receber um erro desconhecido. Os valores possíveis são *Não Conectado*, *Conectado*,

CATEGORIA	MÉTRICAS	DESCRIÇÃO
		Desconhecido e *n/a* (com ícone de ajuda).
Utilização de Recursos	Uso da CPU %	Exibe o uso da CPU em porcentagem usando um gráfico de linha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	CPU Média %	Exibe a porcentagem média de CPU do servidor do Provisioning Service agregada nos últimos 10 minutos.
	Pico de CPU %	Exibe a porcentagem de pico de CPU do servidor do Provisioning Service nos últimos 5 minutos.
	Uso de Memória %	Exibe o uso de memória em porcentagem usando um gráfico de pilha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	Média de Memória %	Exibe a porcentagem média de memória do servidor do Provisioning Service agregada nos últimos 10 minutos.
	Pico de Memória %	Exibe a porcentagem de pico de memória do servidor do Provisioning Service nos últimos 5 minutos.
	IOPS de Disco	Exibe o valor de entrada e saída do disco usando um gráfico de linha.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	Média de IOPS de Disco %	Exibe a média de IOPS de disco do servidor do Provisioning Service agregada nos últimos 10 minutos.
	Pico de IOPS de Disco %	Exibe a porcentagem de pico de IOPS de disco do servidor do Provisioning Service nos últimos 10 minutos.
	Latência do Disco (Ms)	Exibe o valor da latência do disco usando um gráfico de linha.
	Latência Média do Disco %	Exibe a latência média do disco do servidor do Provisioning Service agregada nos últimos 10 minutos.
	Pico de Latência do Disco %	Exibe a porcentagem de pico de latência do disco do servidor do Provisioning Service nos últimos 5 minutos.
Impacto	Total de Logins Rejeitados	Número total de falhas de login dividido pelo número total de tentativas de login.
	Contagem de Dispositivos Ativos	Exibe o número total de dispositivos ativos no servidor do Provisioning Service. Esta métrica é um valor inteiro.

Métricas de saúde do StoreFront™

Clique na guia **Infraestrutura** e selecione **StoreFront**. O painel de Infraestrutura para StoreFront é exibido:



Os seguintes detalhes são monitorados para servidores StoreFront:

CATEGORIA	MÉTRICAS	DESCRIÇÃO
Acessibilidade	Nome do host	Exibe o nome do servidor StoreFront. Esta métrica é um valor de string.
	Status do Servidor	Exibe o status do servidor StoreFront. Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: *Não em execução*, *Em execução*, *Não instalado* e *n/d* (com ícone de ajuda).
	Status da URL Base	Exibe a integridade da URL base. Se o código de status HTTP for 200, o status é UP. Caso contrário, o valor é Down.
	Última Inicialização	Exibe a hora em que o servidor StoreFront foi inicializado pela última vez.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	Última atualização	Exibe a hora em que os dados foram coletados do servidor StoreFront.
Serviços Dependentes	Serviço de Domínio	Integridade do serviço do Windows denominado serviço de domínio. Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: *Não em execução*, *Em execução*, *Não instalado* e *n/a* (com ícone de ajuda).
	Serviço de Carteira de Credenciais	Este serviço é um serviço do Windows usado para armazenar senhas criptografadas. Os valores possíveis são: *Não em execução*, *Em execução*, *Não instalado* e *n/a* (com ícone de ajuda).
	Serviço de Resolução de Pares	Este serviço é um serviço do Windows responsável pela comunicação de rede entre grupos de servidores, formando uma malha de pares de servidores StoreFront. Os valores possíveis são: *Não em execução*, *Em execução*, *Não instalado* e *n/d* (com ícone de ajuda).
	Serviço WWW	Esta métrica é o serviço web do servidor StoreFront. Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: *Não em execução*, *Em execução*,

CATEGORIA	MÉTRICAS	DESCRIÇÃO
		Não instalado e *n/d* (com ícone de ajuda).
Utilização de Recursos	Uso da CPU %	Exibe o uso da CPU em porcentagem usando um gráfico de linha. O valor exibido é o mais recente no final dos últimos cinco minutos.
	Média da CPU %	Exibe a porcentagem média da CPU do servidor StoreFront agregada nos últimos 10 minutos.
	Pico da CPU %	Exibe a porcentagem de pico da CPU do servidor StoreFront nos últimos cinco minutos. Este valor ajuda a decidir a capacidade máxima necessária para uma CPU.
	Uso de Memória %	Exibe o uso da memória em porcentagem usando um gráfico de pilha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	Média de Memória %	Exibe a porcentagem média de memória do servidor StoreFront agregada nos últimos 10 minutos.
	Pico de Memória %	Exibe a porcentagem de pico de memória do servidor StoreFront nos últimos 5 minutos.
	IOPS de Disco	Exibe o valor de entrada e saída do disco usando um gráfico de linha.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	Média de IOPS de Disco %	Exibe a média de IOPS de disco do servidor StoreFront usando um valor flutuante.
	Pico de IOPS de Disco %	Exibe a porcentagem de pico de IOPS de disco do servidor StoreFront agregada nos últimos 10 minutos.
	Latência do Disco (Ms)	Exibe o valor de latência do disco usando um gráfico de linha.
	Latência Média do Disco %	Exibe a latência média do disco do servidor StoreFront agregada nos últimos 10 minutos.
	Pico de Latência do Disco %	Exibe a porcentagem de pico de latência do disco do servidor StoreFront nos últimos cinco minutos.
Impacto	Validade do Certificado ICA®	Exibe a validade do certificado ICA. Os valores possíveis são *Expirado*, *Expirando*, *Válido* e *Não Encontrado*.
	Validade da Cadeia de Certificados ICA	Exibe se a Cadeia de Certificados ICA do StoreFront é válida ou não. O valor possível é *Sim* ou *Não*.
	Validade do Certificado IIS	Exibe a validade do certificado IIS. Os valores possíveis são *Expirado*, *Expirando*, *Válido* e *Não Encontrado*.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	Validade da Cadeia de Certificados IIS	Exibe se a Cadeia de Certificados IIS do StoreFront é válida ou não. O valor possível é *Sim* ou *Não*.

Métricas de saúde do Cloud Connector

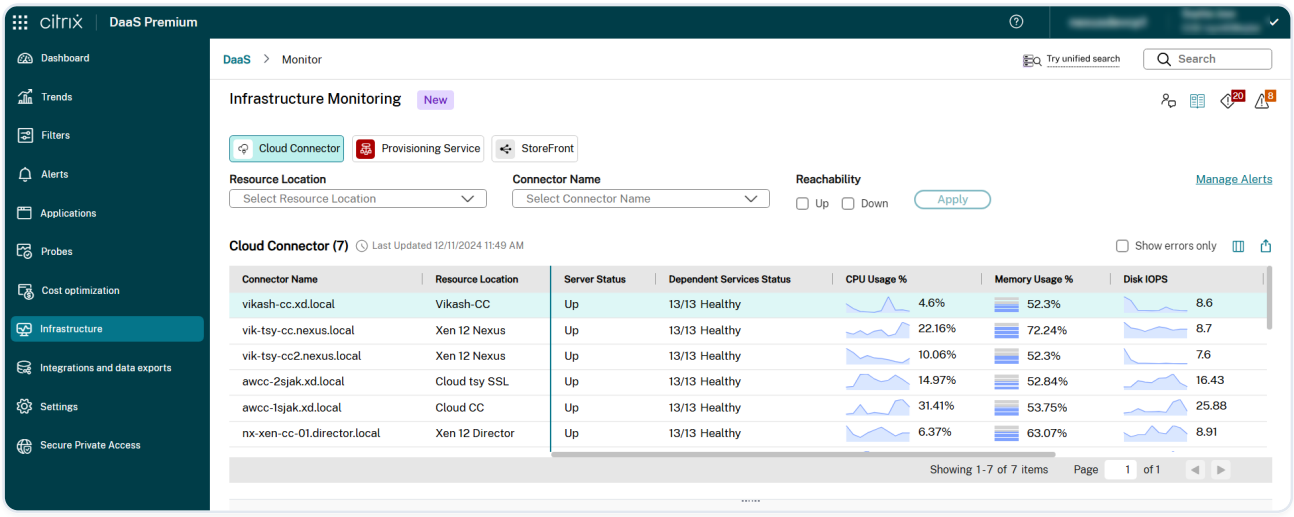
O componente Cloud Connector é adicionado por padrão como parte do monitoramento de infraestrutura. O componente Cloud Connector que está conectado ao site Citrix DaaS™ é automaticamente integrado para monitoramento.

Este recurso permite que os clientes monitorem a saúde do Cloud Connector no painel de monitoramento de infraestrutura e configurem alertas para ele. A funcionalidade de alerta permite que os administradores de clientes sejam alertados se alguma das políticas criadas para os Cloud Connectors estiver em estágio crítico ou de aviso.

Você pode selecionar o tipo de **Componente** necessário e os detalhes são exibidos de acordo com o nome do site selecionado. Você também pode selecionar o **Local do recurso**.

> **Nota:**
>
> O arquivo `citrixinframonitor.msi` não é necessário para monitorar os Cloud Connectors.
>
> Você pode monitorar detalhes de infraestrutura de site único e de múltiplos sites.

Clique na guia **Infraestrutura** e selecione **Cloud Connector**. O painel de infraestrutura para Cloud Connector aparece:



Os seguintes detalhes são monitorados para o Cloud Connector:

CATEGORIA	MÉTRICAS	DESCRIÇÃO
Acessibilidade	Status do Servidor	Mostra o estado de acessibilidade do Cloud Connector fornecido. Os valores possíveis são *Ativo* e *Inativo*.
	Status do Serviço Dependente	Fornece o resumo do status do Serviço Dependente do Cloud Connector. Os valores possíveis são **13/13 Em Execução** (quando todos os serviços estão em execução) ou `<number of stopped services>/13 Not Running` (mostra os serviços que não estão em execução na dica de ferramenta).
	Versão	A versão do Cloud Connector.
	Hora da Última Inicialização	Exibe a hora em que o Cloud Connector foi inicializado pela última vez.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	Última atualização	Exibe a última hora em que os dados foram coletados do Cloud Connector.
Serviços Dependentes-Esta métrica mostra o status dos serviços do Windows. Os valores possíveis são: Desconhecido, Não em execução, Inicialização Pendente, Parada Pendente, Em execução, Continuação Pendente, Pausa Pendente, Pausado e Não Instalado.	Serviço Citrix Connection Lease Exchange	Exibe o status do serviço Citrix Connection Lease Exchange, que permite que os arquivos de Connection Lease sejam trocados entre o aplicativo Citrix Workspace™ e o Cloud Connector para Service Continuity for Workspace.
	Citrix AD Provider	Exibe o status do serviço Citrix AD Provider, que permite que o Citrix Cloud™ facilite o gerenciamento de recursos associados às contas de domínio do Active Directory nas quais ele está instalado.
	Citrix Agent Discovery	Exibe o status do serviço Citrix Agent Discovery que permite ao Citrix Cloud facilitar o gerenciamento de produtos Citrix locais legados XenApp e XenDesktop®.
	Citrix Credential Provider	Exibe o status do Citrix Credential Provider que lida com o armazenamento e a recuperação de dados criptografados.
	Citrix NetScaler® Cloud Gateway	Exibe o status do Citrix NetScaler Cloud Gateway que fornece conectividade com a Internet para desktops e aplicativos locais sem a

CATEGORIA	MÉTRICAS	DESCRIÇÃO
		necessidade de abrir regras de firewall de entrada ou implantar componentes na DMZ.
	Citrix Agent Logger	Exibe o status do Citrix Agent Logger que fornece uma estrutura de log de suporte para os serviços do Citrix Cloud Connector™.
	Citrix WebRelay Provider	Exibe o status do Citrix WebRelay Provider que permite que as solicitações HTTP recebidas do serviço WebRelay Cloud sejam encaminhadas para servidores Web locais.
	Serviço de Alta Disponibilidade Citrix	Exibe o status do serviço Citrix High Availability que fornece continuidade de serviço durante a interrupção de um site central.
	Servidor HCL Remoto Citrix	Exibe o status do Servidor HCL Remoto Citrix que atua como proxy para comunicações entre o Delivery Controller™ e os Hypervisors.
	Provedor de Broker Remoto Citrix	Exibe o status do Provedor de Broker Remoto Citrix que permite a comunicação com um Serviço de Broker remoto a partir de VDAs locais e servidores StoreFront.
	Serviço de Captura CDF Citrix	Exibe o status do serviço de Captura CDF Citrix que captura rastreamentos CDF

CATEGORIA	MÉTRICAS	DESCRIÇÃO
		de todos os produtos e componentes configurados.
	Sincronizador de Configuração Citrix	Exibe o status do Sincronizador de Configuração Citrix que copia a configuração de corretagem localmente para o modo de alta disponibilidade.
	WatchDog do Agente Citrix	Exibe o status do Citrix Agent WatchDog, que monitora e atualiza os agentes locais (evergreen).
Utilização de Recursos	Uso da CPU %	Exibe o uso da CPU em porcentagem usando um gráfico de linha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	Média da CPU %	Exibe a porcentagem média da CPU do servidor Cloud Connector agregada nos últimos 10 minutos.
	Pico da CPU %	Exibe a porcentagem de pico da CPU do servidor Cloud Connector nos últimos 5 minutos.
	Uso da Memória %	Exibe o uso da memória em porcentagem usando um gráfico de pilha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	Média da Memória %	Exibe a porcentagem média de memória do servidor

CATEGORIA	MÉTRICAS	DESCRIÇÃO
		Cloud Connector agregada nos últimos 10 minutos.
	Pico de Memória %	Exibe a porcentagem de pico de memória do servidor Cloud Connector nos últimos 5 minutos.
	IOPS de Disco	Exibe o valor de entrada e saída do disco usando um gráfico de linha.
	Média de IOPS de Disco %	Exibe a média de IOPS de disco do servidor Cloud Connector agregada nos últimos 10 minutos.
	Pico de IOPS de Disco %	Exibe a porcentagem de pico de IOPS de disco do servidor Cloud Connector nos últimos 10 minutos.
	Latência do Disco (Ms)	Exibe o valor de latência do disco usando um gráfico de linha.
	Latência Média do Disco %	Exibe a latência média do disco do servidor Cloud Connector agregada nos últimos 10 minutos.
	Latência Máxima do Disco %	Exibe a porcentagem de latência máxima do disco do servidor Cloud Connector nos últimos 5 minutos.

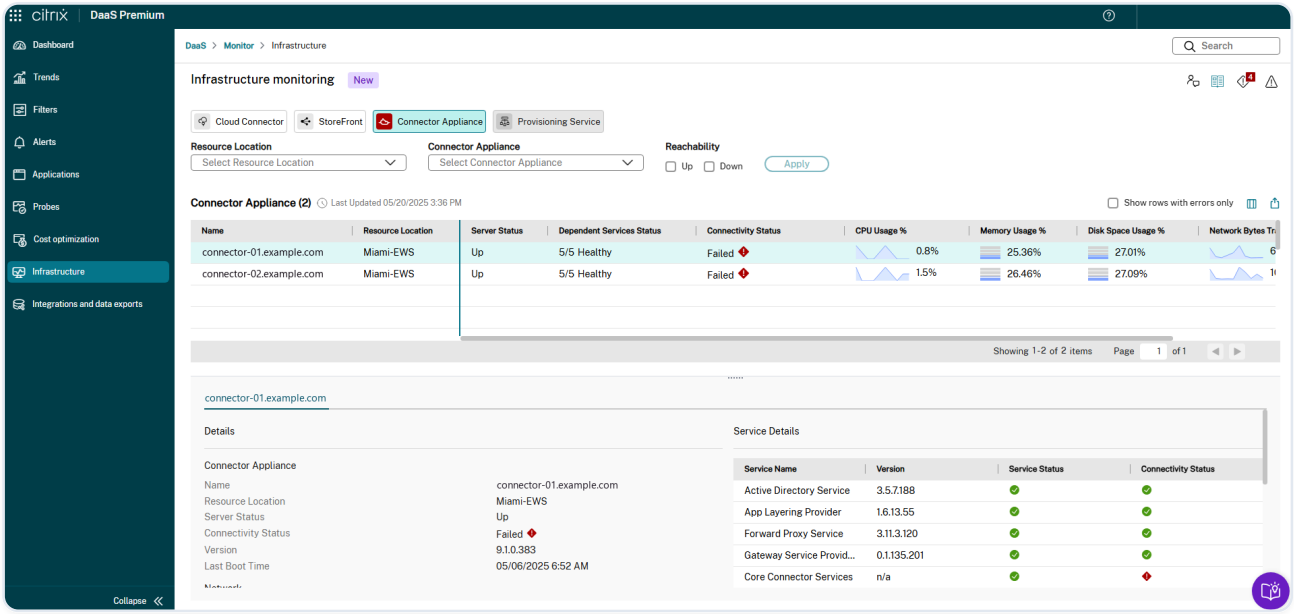
Métricas de saúde do Connector Appliance

O componente **Connector Appliance** é adicionado por padrão como parte do monitoramento de infraestrutura. O componente **Connector Appliance** que está conectado ao site Citrix DaaS é automaticamente integrado para monitoramento.

Este recurso permite que os clientes monitorem a saúde do Connector Appliance no painel de monitoramento de infraestrutura.

Você pode selecionar o tipo de **Componente** necessário e os detalhes são exibidos de acordo com o nome do site selecionado. Você também pode selecionar o **Local do recurso**.

Clique na guia **Infraestrutura** e selecione **Connector Appliance**. O painel de infraestrutura para Connector Appliance é exibido:



Os seguintes detalhes são monitorados para o Connector Appliance:

CATEGORIA	MÉTRICAS	DESCRIÇÃO
Acessibilidade	Status do Servidor	Mostra o estado de acessibilidade do Connector Appliance fornecido. Os valores possíveis são *Ativo* e *Inativo*. O Connector Appliance envia eventos de status para a Citrix a cada 5 minutos, o estado *Inativo* ocorre quando nenhum evento foi recebido por 20 minutos consecutivos.
	Status do Serviço Dependente	Fornece o resumo do status do Serviço Dependente do Connector Appliance. Os valores possíveis são **5/5 Em**

CATEGORIA	MÉTRICAS	DESCRIÇÃO
		Execução (quando todos os serviços estão em execução) ou `<stopped>/5 Not Running`.
	Status de Conectividade	Exibe se o serviço pode alcançar os endereços no Citrix Cloud necessários para sua operação. Os valores possíveis são *Sucesso* e *Falha*.
	Versão	A versão do Connector Appliance.
	Última Inicialização	Exibe a hora em que o Connector Appliance foi inicializado pela última vez.
	Última atualização	Exibe a última hora em que os dados foram coletados do Connector Appliance.
	Detalhes do Proxy	Exibe o proxy que o Connector Appliance usa.
Rede	IP Público v4	Exibe o endereço IP público do Connector Appliance.
	IP Privado	Exibe o endereço IP privado do Connector Appliance.
Autenticação	AD Configurado	*Verdadeiro* ou *Falso* para indicar se o Servidor Connector Appliance configurou o AD.
	Domínios unidos	Exibe o domínio ao qual o Connector Appliance se uniu.
Serviços Dependentes	Serviço Active Directory	Permite a integração com o Active Directory,

CATEGORIA	MÉTRICAS	DESCRIÇÃO
		possibilitando a autenticação e o gerenciamento de usuários em vários domínios.
	Provedor de App Layering	Conecta o appliance Citrix App Layering™ ao Active Directory, permitindo junções de diretório para gerenciar atributos de usuário.
	Serviço Gateway	Facilita o acesso seguro aos serviços Citrix Cloud, garantindo conectividade contínua entre recursos locais e ambientes de nuvem.
	Serviço de Proxy de Encaminhamento	Ajuda a gerenciar conexões de saída, garantindo comunicação segura e eficiente entre o Citrix Cloud e as redes corporativas.
	Serviços de Conector Principais	Permite a comunicação entre o Citrix Cloud e os locais de recursos, suportando autenticação, portabilidade de imagem e outras funções de gerenciamento de nuvem.
Utilização de Recursos	Uso da CPU %	Exibe o uso da CPU em porcentagem usando um gráfico de linha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	Média da CPU %	Exibe a porcentagem média da CPU do servidor Connector Appliance agregada nos últimos 10 minutos.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	Pico da CPU %	Exibe a porcentagem de pico da CPU do servidor Connector Appliance nos últimos 10 minutos.
	Uso da Memória %	Exibe o uso da memória em porcentagem usando um gráfico de pilha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	Média de Memória %	Exibe a porcentagem média de memória do servidor Connector Appliance agregada nos últimos 10 minutos.
	Pico de Memória %	Exibe a porcentagem de pico de memória do servidor Connector Appliance nos últimos 10 minutos.
	Uso do Espaço em Disco %	Exibe o uso do espaço em disco em porcentagem usando um gráfico de pilha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	Média de Uso do Espaço em Disco %	Exibe a porcentagem média de uso do espaço em disco do servidor Connector Appliance agregada nos últimos 10 minutos.
	Pico de Uso do Espaço em Disco %	Exibe a porcentagem de pico de uso do espaço em disco do servidor Connector Appliance nos últimos 10 minutos.

CATEGORIA	MÉTRICAS	DESCRIÇÃO
	Bytes de Rede Transferidos Por Minuto	Exibe os bytes de rede transferidos por minuto usando um gráfico de linha. O valor exibido é o mais recente no final dos últimos 5 minutos.
	Média de Bytes de Rede Transferidos Por Minuto	Exibe a média de bytes de rede transferidos por minuto do servidor Connector Appliance nos últimos 10 minutos.
	Pico de Bytes de Rede Transferidos Por Minuto	Exibe o pico de bytes de rede transferidos por minuto do servidor Connector Appliance nos últimos 10 minutos.

Criar e gerenciar alertas

Você pode configurar alertas para monitorar proativamente condições e escopos de seu interesse e reduzir a fadiga de alertas. Os alertas podem ser configurados com severidade, intervalos de re-alerta, meios de notificação e seguem o ciclo de vida do alerta suportado no produto.

Para obter mais informações, consulte o seguinte:

- Alertas
- Políticas de alerta avançadas

Sondagem de Aplicativos e Desktops

A sondagem de aplicativos e desktops automatiza o processo de verificação da integridade dos aplicativos e desktops publicados em um site, iniciando-os sequencialmente para teste usando o StoreFront. Os resultados da sondagem estão disponíveis no console **Monitor** do Citrix DaaS. O Citrix Probe Agent oferece suporte a todos os sites, incluindo aqueles hospedados no Citrix Cloud™ Japan e nos Planos de Controle do Citrix Cloud Government.

Requisitos

- As máquinas de endpoint que executam agentes de sondagem são máquinas Windows com o aplicativo Citrix Workspace™ para Windows versão 1808 ou posterior para sondagem de aplicativos e versão 1906 ou posterior para sondagem de desktops. O aplicativo Workspace para Unified Windows Platform (UWP) não é compatível.
- O Citrix Probe Agent oferece suporte à autenticação padrão baseada em formulário, conforme suportado pelo Citrix® StoreFront Cloud. Nos casos em que o dispositivo de endpoint está conectado a uma loja usando o Citrix Gateway, você pode autenticar usando as credenciais de domínio do Citrix Gateway ou autenticação multifator (MFA). O Citrix Probe Agent não oferece suporte a outros métodos de autenticação, como Single Sign-On (SSO). Da mesma forma, o Citrix Probe Agent funciona apenas quando não há servidor proxy ou balanceador de carga como Citrix Gateway ou Citrix ADC implantado.
- A sondagem de aplicativos e desktops está disponível no Citrix DaaS™ Premium e no Citrix DaaS Premium Plus.

  > **Nota:**
  >
  > - Se o usuário ativou a política de login ou autenticação condicional no Citrix Cloud, o agente de sondagem falha ao fazer login no Storefront™ ou no aplicativo Citrix Workspace.
  > - O Probe Agent oferece suporte apenas à autenticação do Active Directory para autenticar no aplicativo Citrix Workspace.

- Certifique-se de que o Microsoft .NET Framework versão 4.7.2 ou posterior esteja instalado na máquina de endpoint onde você deseja instalar o Probe Agent.
- Para usar o agente de sondagem no Plano de Controle do Citrix Cloud Japan, defina o valor do registro no caminho “\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region” como 2. Para usar o agente de sondagem no Plano de Controle do Citrix Cloud Government, defina o valor do registro no caminho “\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region” como 3.

Contas de usuário/permissões necessárias para executar a Sondagem:

- Um usuário exclusivo para sondar em cada máquina de endpoint. O usuário não precisa ser um administrador; as sondagens podem ser executadas em um contexto não administrativo.
- Contas de usuário com permissões de administrador do Windows para instalar e configurar o Citrix Probe Agent nas máquinas de endpoint.
- O usuário deve ser membro do mesmo domínio que os VDAs usados para o lançamento de aplicativos ou desktops. O Probe Agent atualmente não oferece suporte a vários domínios.
- Reutilizar contas de usuário existentes para sondagem pode desconectar os usuários de suas sessões ativas. Uma conta de usuário administrador completa ou uma função personalizada com as seguintes permissões:
    - Permissões de grupo de entrega:
        - Somente leitura
    - Permissões do Director:
        - Criar\\Editar\\Remover Configuração do Servidor de E-mail de Alerta - se o servidor de e-mail ainda não estiver configurado
        - Criar\\Editar\\Remover Configurações de Sondagem
        - Visualizar página de Configurações
        - Visualizar página de Tendências

Configuração

Você pode agendar suas sondagens para serem executadas durante o horário de pico em várias regiões geográficas. Os resultados abrangentes da sondagem podem ajudar a solucionar problemas relacionados aos aplicativos, máquina de hospedagem ou conexão antes que os usuários os experimentem.

O Citrix Probe Agent versão 2103 suporta agregação de sites. Aplicativos e desktops podem ser enumerados e iniciados a partir de sites agregados. Ao configurar o agente de sondagem, selecione a opção **Agregação de Sites do Workspace (StoreFront) Ativada** para habilitar a enumeração de aplicativos e desktops de sites agregados. As seguintes combinações de sites são suportadas:

- Vários sites locais com uma URL de loja.
- Sites locais e na nuvem com uma URL de loja local ou uma URL de loja na nuvem.
- Vários sites na nuvem com uma URL de loja.

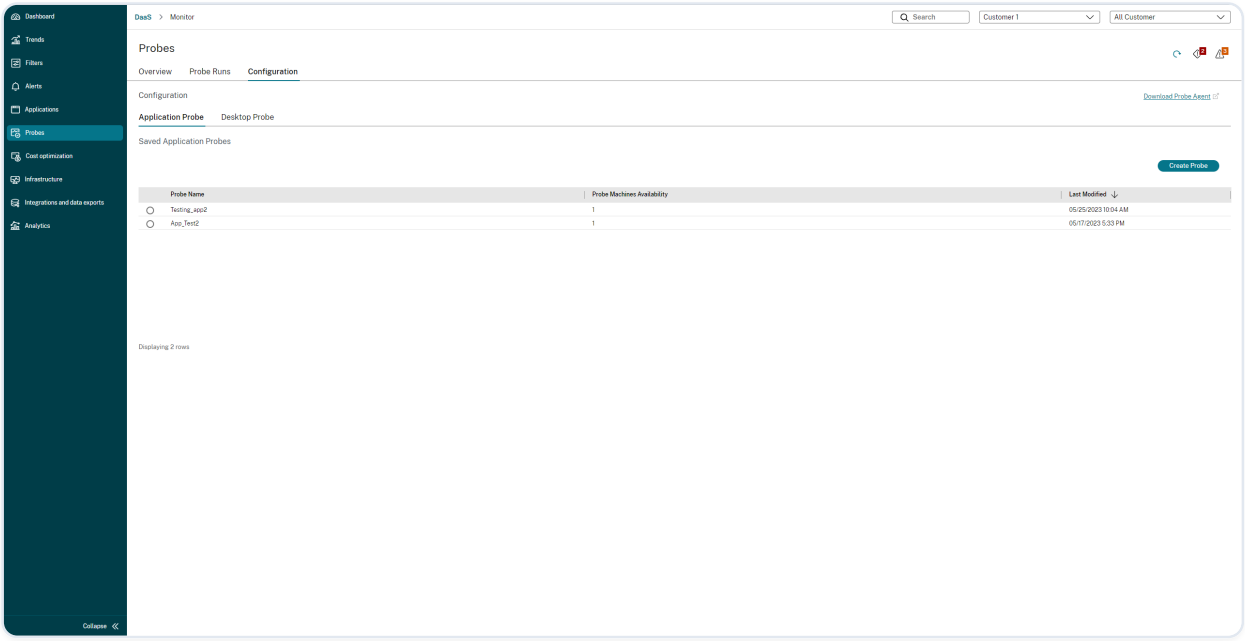
Nota:

Você deve criar administradores ou usuários separados para configurar sondas que tenham acesso a apenas um site.

Etapa 1: Instalar e configurar o Citrix Probe Agent

O Citrix Probe Agent é um executável do Windows que simula o lançamento real de aplicativos ou desktops pelo usuário através do StoreFront. Ele testa os lançamentos conforme configurado no Monitor e reporta os resultados de volta ao Monitor.

1. Identifique as máquinas de endpoint de onde você deseja executar a sondagem.
2. Usuários com privilégios administrativos podem instalar e configurar o Citrix Probe Agent na máquina de endpoint. Baixe o executável do Citrix Probe Agent disponível na página downloads da Citrix.

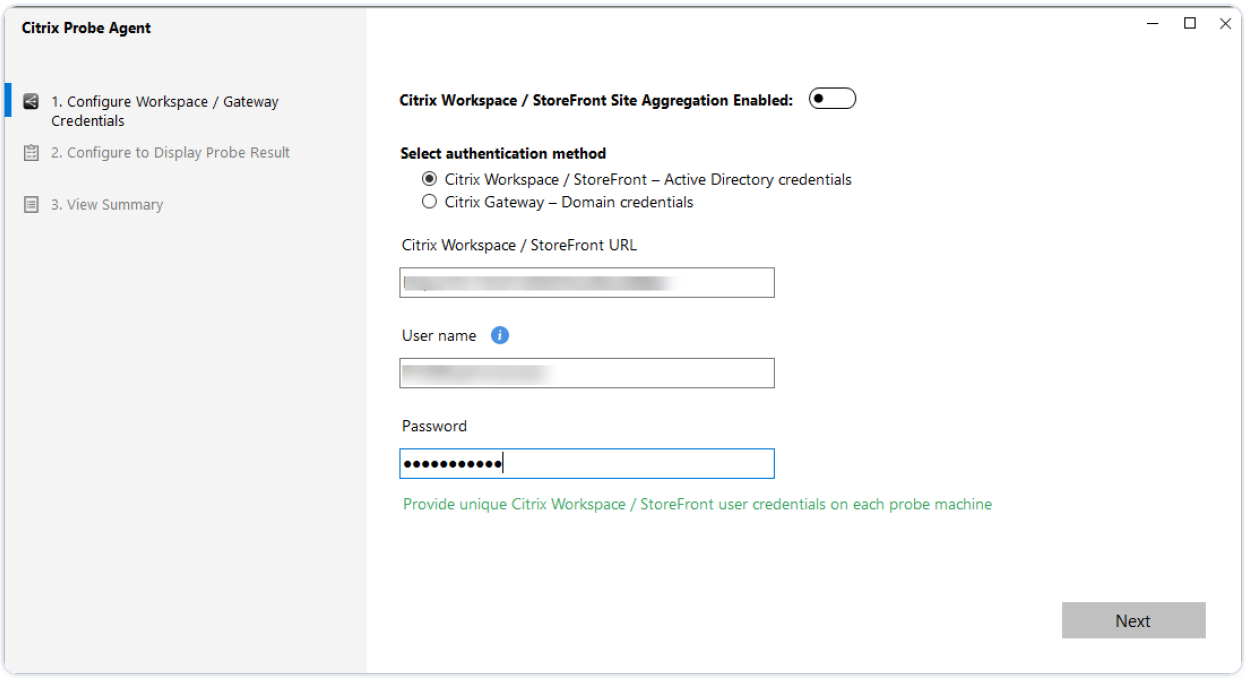


3. Inicie o agente e insira as credenciais de um usuário apropriado. Configure um usuário exclusivo em cada máquina de endpoint. As credenciais são criptografadas e armazenadas com segurança.

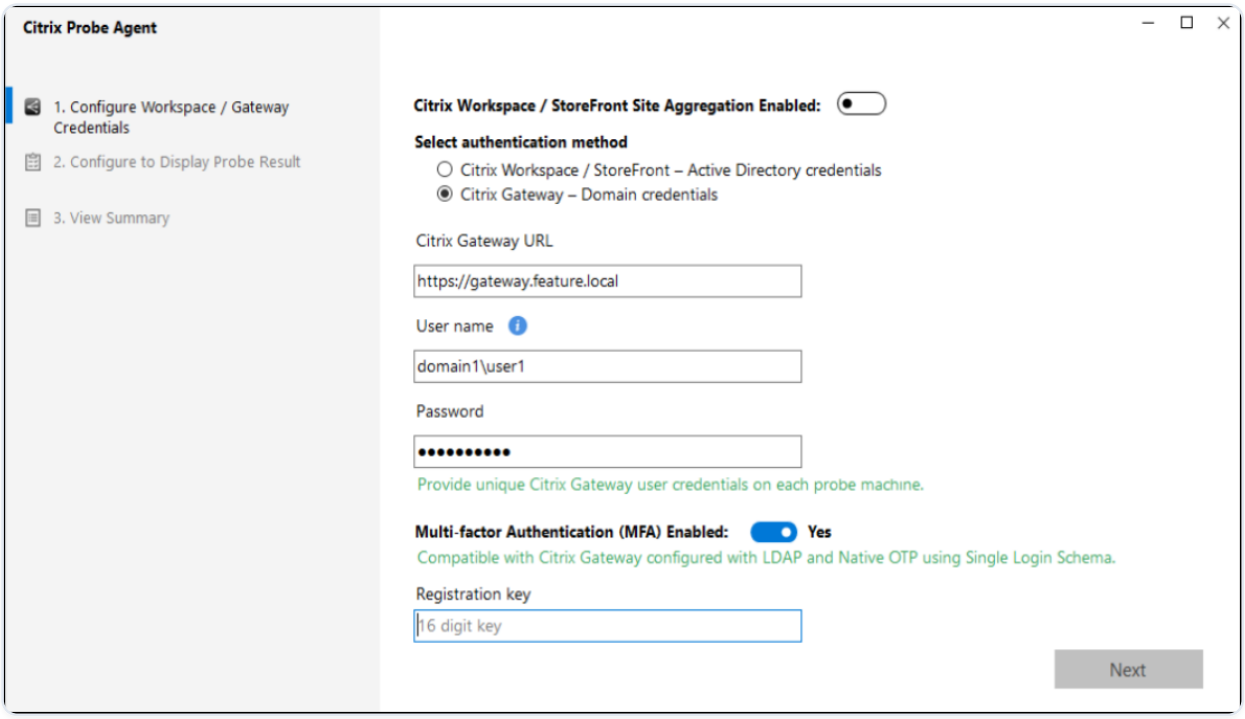
Observações:

- Para acessar o site a ser sondado de fora da rede, digite a URL de login para o Citrix Gateway no campo **URL da loja**. O Citrix Gateway roteia automaticamente a solicitação para a URL da loja do site correspondente.
- Use NetBIOS como o nome de domínio no campo de nome de usuário. Por exemplo, NetBIOS/nome de usuário.
- A sondagem de aplicativos suporta o serviço Citrix Content Collaboration™ usando autenticação (somente AD).

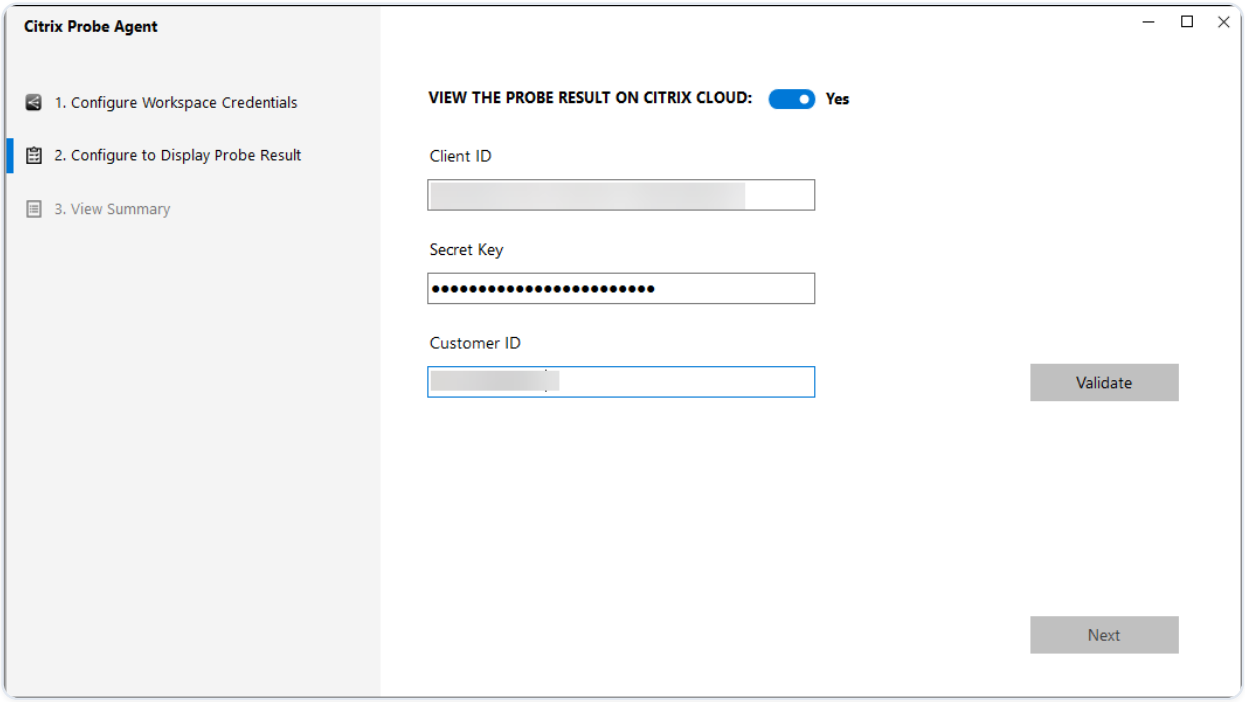
4. Selecione um método de autenticação e insira as credenciais relevantes. As credenciais são criptografadas e armazenadas com segurança.
5. Configure com suas credenciais do StoreFront Active Directory. Configure um usuário exclusivo em cada máquina de endpoint.



6. Escolha a opção Citrix Gateway se seu endpoint estiver conectado ao StoreFront via Citrix Gateway e configure com suas credenciais de Domínio do Citrix Gateway.



7. Escolha a opção de Autenticação Multifator se o seu Gateway a suportar e insira a chave de autenticação de 16 dígitos. Isso está disponível apenas para o Citrix Gateway configurado com LDAP e OTP Nativo usando o Esquema de Login Único.
8. Na guia **Configurar para Exibir Resultado da Sondagem**, insira as credenciais para acessar o Citrix DaaS. Você pode encontrar o Nome do Cliente ou ID do Cliente, ID do Cliente e Chave Secreta na página Acesso à API no console do Citrix Cloud.



9. Selecione seu site e clique em Avançar.

10. Na guia **Visualizar Resumo**, certifique-se de que os detalhes configurados estejam precisos. Se precisar fazer alterações, vá para a guia respectiva e faça as atualizações.

Etapa 2: Configurar Sondagem no Monitor

> **Limitação:**

> A sondagem falha se aplicativos ou desktops forem iniciados para teste a partir de VDAs Windows que têm o banner de mensagem de logon interativo ativado. Isso ocorre porque um tempo limite é atingido devido à espera para aceitar a mensagem de logon interativo. Para desativar a mensagem de logon em um VDA de Servidor. Vá para Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas Locais > Opções de Segurança.

> Remova o texto nos seguintes campos e atualize a política da Microsoft.

> - Logon Interativo: Texto da Mensagem para usuários tentando fazer logon
> - Logon Interativo: Título da Mensagem para usuários tentando fazer logon

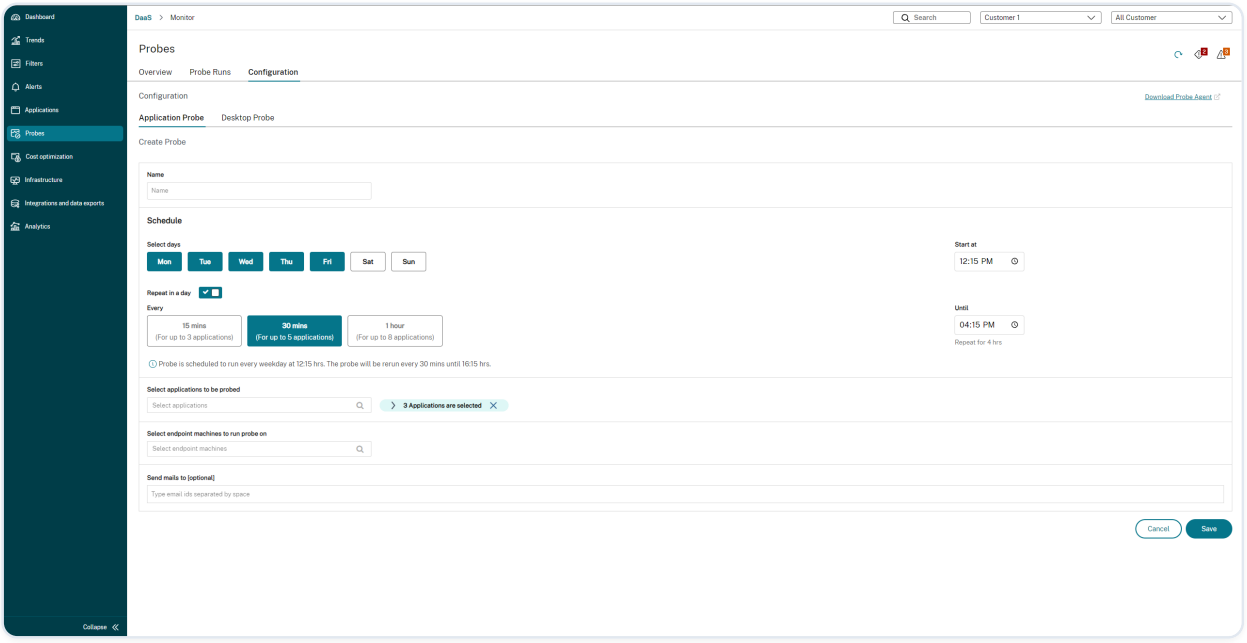
> Atribua o usuário de sondagem a este VDA de Servidor específico com o banner de mensagem de logon interativo desativado para garantir que a sondagem possa passar do Estado de Lançamento de Aplicativo ou Desktop.

> Para obter mais informações, consulte `<https://learn.microsoft.com/pt-br/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`.

1. Vá para **Configuração** \> **Configuração da Sondagem** \> **Sondagem de Aplicativo** ou **Sondagem de Desktop** e clique em **Criar Sondagem**.
2. Na página **Criar Sondagem**, insira o nome da sondagem.
3. Selecione o agendamento:
    a. Escolha os dias da semana em que você deseja que a sondagem seja executada.
    b. Insira a hora de início em que você deseja que a sondagem seja executada.

c. Além disso, você pode escolher a opção **Repetir em um dia**. Insira a hora de término e o intervalo em que você deseja que a sondagem se repita dentro de um dia. Por exemplo, a configuração abaixo ajuda a executar sondagens de aplicativos das 12:08 horas até as 16:34 horas, repetindo a cada 30 minutos todas as segundas, quartas, quintas e domingos.

4. Selecione o número recomendado de aplicativos ou desktops a serem sondados, dependendo do intervalo.
5. Selecione as máquinas de endpoint nas quais a sondagem deve ser executada.
6. Insira os endereços de e-mail para os quais os resultados da sondagem de falha são enviados. Configure seu servidor de e-mail em **Alertas** > **Configuração do Servidor de E-mail**.



Nesta configuração, as sessões do aplicativo são iniciadas às 12:08, 12:38, 13:08 e assim por diante até as 16:08, todas as segundas, quartas, quintas e domingos.

Nota:

- Após a configuração, o agente executa as sondagens configuradas a partir da próxima hora.
- As sondagens que foram configuradas antes da introdução da opção **Repetir em um dia** continuam a ser executadas no horário agendado. Elas têm a opção **Repetir em um dia** desativada por padrão.

- Recomenda-se que você configure as sondagens de forma que cada execução tenha um período de 5 minutos para evitar sobreposições.

Etapa 3: Execução da sondagem

O agente executa a sondagem de acordo com a configuração da sonda que ele busca do Monitor periodicamente. Ele inicia aplicativos ou desktops selecionados serialmente usando o Workspace. O agente reporta os resultados de volta ao Monitor via banco de dados do Monitor. As falhas são reportadas em cinco estágios específicos:

- **Acessibilidade do Workspace** - a URL da loja configurada não está acessível.
- **Autenticação do Workspace** - as credenciais do StoreFront configuradas são inválidas.
- **Enumeração do Workspace** - a lista de aplicativos enumerados do Workspace não contém o aplicativo ou desktop a ser sondado.
- **Download do ICA®** - o arquivo ICA não está disponível.
- **Inicialização de Aplicativo / Desktop** – o aplicativo ou desktop não pôde ser iniciado.

Etapa 4: Visualizar resultados da sonda

Você pode ver os resultados da sonda em **Sondas**. A visualização Sondas oferece uma visão abrangente dos resultados da sonda. Esses resultados ajudam a analisar e solucionar problemas proativamente, permitindo uma experiência de inicialização de sessão mais suave para os usuários.

A guia **Visão Geral** fornece um resumo de todas as sondas configuradas em uma única visualização.

Execuções da sonda do Monitor(/en-us/citrix-daas/media/dir-probe-metrics-chart.png)

Você pode filtrar sondas com base em Período de Tempo, Tipo de Sonda, Nome do Endpoint, Nome do Aplicativo, Nome do Desktop e Tipo de Resultado da Sonda. As sondas que correspondem aos critérios de filtro são mostradas com os seguintes detalhes por sonda, aplicativo/desktop e endpoint.

Métricas da Sonda mostra a contagem de execuções Agendadas, Planejadas, Ignoradas, Bem-sucedidas e Falhas.

- Execuções Concluídas – o número de execuções da sonda que foram concluídas.
- Execuções com Falha – o número de execuções da sonda que falharam.

- Execuções Ignoradas – O número de execuções ignoradas é igual ao número de execuções agendadas menos a soma das execuções com falha e das execuções bem-sucedidas.
- Execuções Bem-sucedidas – o número de sondas que foram concluídas com sucesso, sem falhas em nenhuma etapa durante o lançamento do aplicativo/desktop.

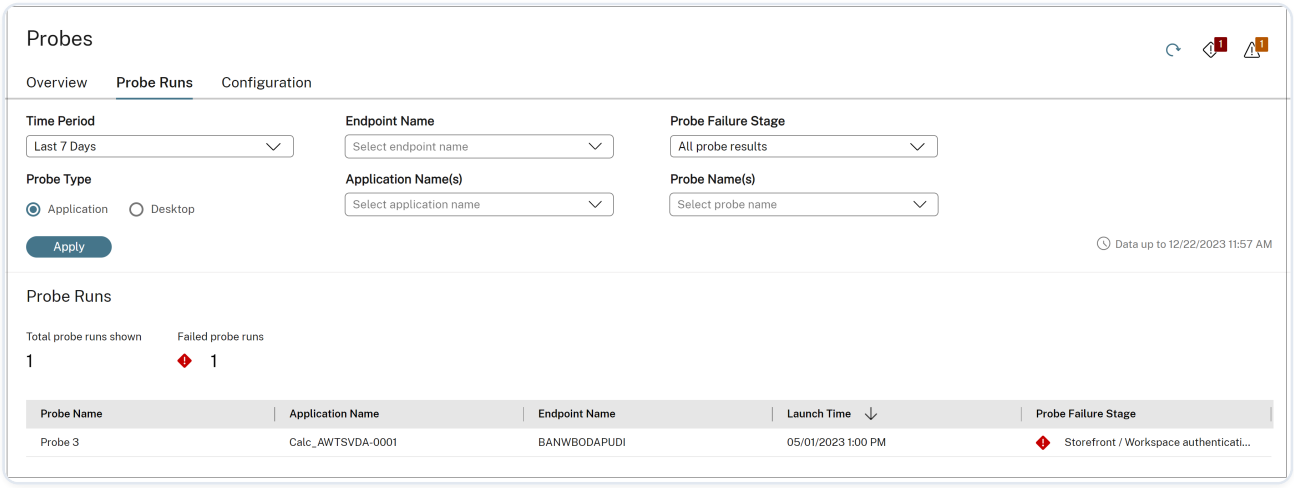
O número total de máquinas de endpoint também é exibido, com a contagem de máquinas ativas e inativas.

Estágios de Falha da Sonda apresenta uma análise visual da distribuição de falhas para cada grupo de falhas. Ao analisar os estágios em que a maioria das falhas ocorreu, torna-se mais fácil interpretar os resultados da sonda e solucionar problemas. A representação gráfica mostra o número de execuções de sonda com falha para o lançamento de aplicativo/desktop, downloads de arquivos ICA, enumeração do Storefront/Workspace, acessibilidade do Storefront/Workspace e autenticação do Storefront/Workspace.

Ajuda a analisar os estágios em que a maioria das falhas ocorreu. Essas informações ajudam a entender rapidamente os resultados da sonda e a solucionar problemas.

Algumas execuções de sonda podem não ser concluídas devido ao endpoint estar inativo ou aos serviços estarem indisponíveis.

A guia **Execuções de Sonda** fornece os resultados das execuções de sonda concluídas em detalhes. Você pode detalhar para ver os detalhes de cada execução individual de uma sonda selecionada. Você pode filtrar e analisar ainda mais com base em pontos de pivô importantes.



Você pode filtrar as execuções de sondas com base em Período de Tempo, Tipo de Sonda, Nome do Endpoint, Nome do Aplicativo, Nome do Desktop e Estágio de Falha da Sonda. O Estágio de Falha da Sonda exibe o estágio em que a sonda falhou. Clicar nos links Nome da Sonda, Execuções Agendadas, Execuções com Falha, Nome do Aplicativo/Desktop também o leva à

página Execuções de Sonda com a lista de execuções de sonda que correspondem aos critérios de filtro.

Otimização de custos

O Citrix Monitor agora apresenta um novo recurso chamado Otimização de Custos, que ajuda a analisar o uso de máquinas virtuais e sessões de forma eficaz. Este recurso fornece representações visuais perspicazes sobre como otimizar o custo. Ele também ajuda a eliminar máquinas desnecessárias e, assim, reduzir os custos.

Para apoiar a otimização de custos, os seguintes alertas também foram introduzidos:

- Ação de ligar falhou e Ação de desligar falhou
- Alerta de tempo de atividade da máquina

Você também pode inspecionar máquinas com ações de energia recentes para analisar falhas de inicialização que causam problemas ao usuário e falhas de desligamento que aumentam os custos. Para obter mais informações, consulte a seção Inspecionar máquinas com ações de energia recentes.

Clique na guia **Otimização de Custos** no menu esquerdo da página **Início** para acessar a página **Otimização de Custos**.



Na página inicial de **Otimização de Custos**, você pode fazer o seguinte:

- Link de introdução - Acesse este link para saber mais sobre o recurso de otimização de custos.
- Revisar a página de otimização de custos - Você pode fornecer feedback sobre a página **Otimização de Custos**
- Atualizar os dados.
- Visualizar os alertas - Você pode visualizar alertas críticos e de aviso.
- Exportar dados

A página **Otimização de Custos** inclui os seguintes recursos:

- Economia de custos
- Dimensionamento correto da carga de trabalho

Como o custo é calculado para otimização de custos

O custo por máquina por hora é exibido na moeda que o hipervisor suporta. Esta seção descreve como o custo é calculado para máquinas Azure e para outras máquinas.

Custo para máquinas Azure

A ordem de prioridade para calcular o custo é a seguinte:

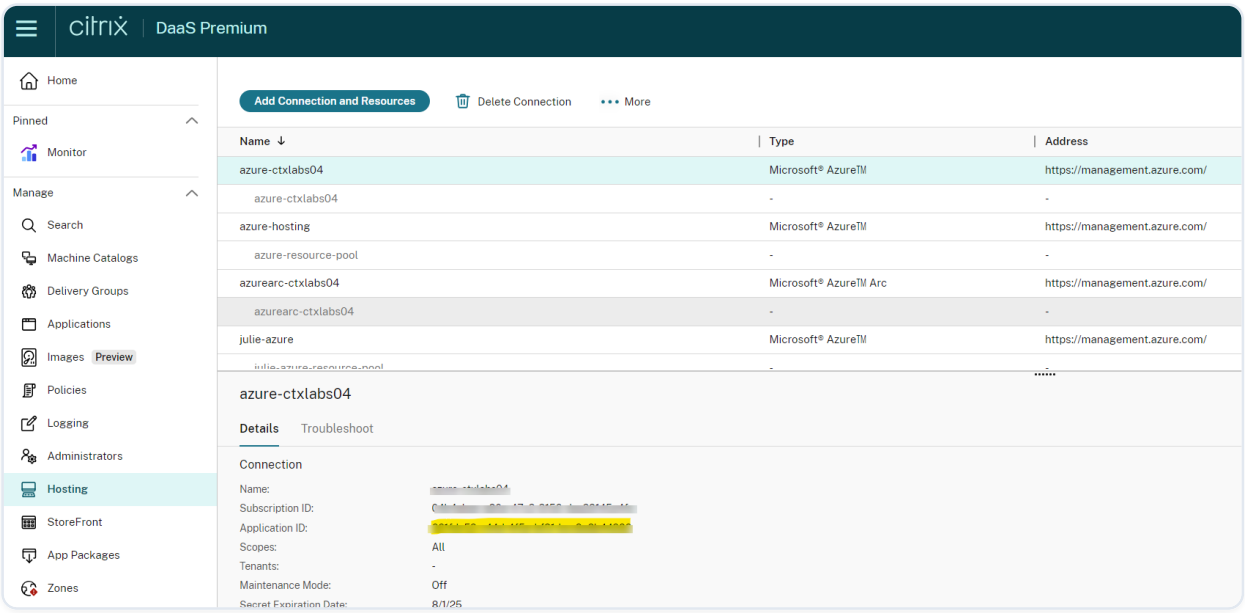
1. Quando a permissão 'Microsoft.Consumption/pricesheets/read estiver disponível, o preço efetivo é exibido na moeda configurada na assinatura do Azure. Este método para calcular o custo está em pré-visualização.
2. Se as permissões não estiverem disponíveis, o preço de varejo do Azure será exibido. Para obter mais informações, consulte Visão geral dos preços de varejo do Azure.

   > **Nota:**
   >
   > Certifique-se de ter acesso ao endpoint `https://prices.azure.com` para permitir a recuperação dos detalhes do preço efetivo ou do preço de varejo.

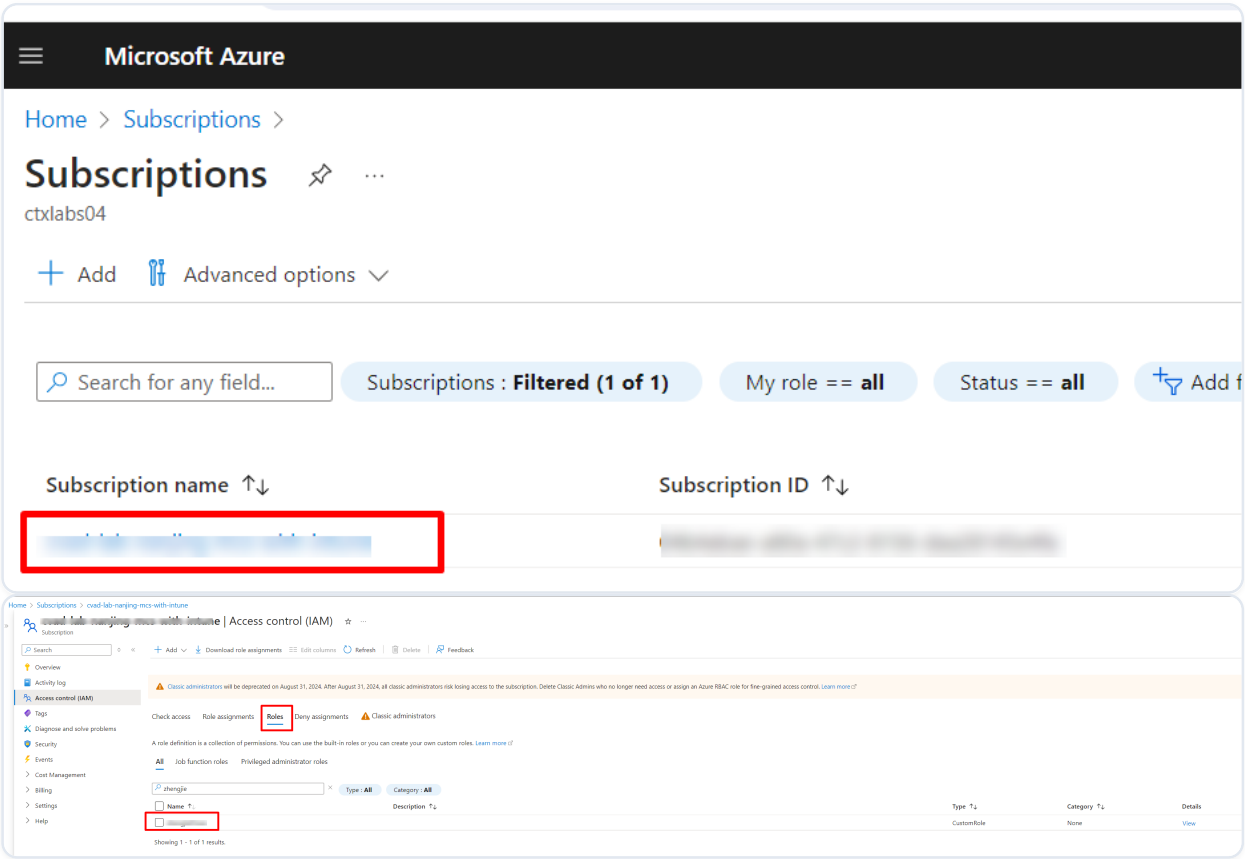
3. Quando o preço efetivo ou o preço de varejo não estiver disponível, o custo é exibido com base no custo inserido pelos administradores no Web Studio. Para obter mais informações, consulte a seção Custo da máquina da documentação.
4. Se nenhum custo for mencionado no Web Studio, o custo padrão de US$ 1 é considerado.

Para encontrar os detalhes da conta do Azure e adicionar a permissão necessária para encontrar o preço efetivo, faça o seguinte:

1. navegar para o Citrix DaaS.
2. Clique na guia **Hospedagem** para encontrar a conta de conexão de hospedagem.
3. Procure o **ID do Aplicativo** mencionado na guia **Hospedagem**.



4. Vá para o Microsoft Entra ID e procure o **ID do Aplicativo** anotado na etapa 3.
5. Vá para **Assinatura** > **Controle de acesso (IAM)** > escolha uma função personalizada configurada para o SPN de conexão de hospedagem.



6. Adicione a permissão *Microsoft.Consumption/pricesheets/read* à função.

Como verificar o preço de varejo do Azure

Se o `Microsoft.Consumption/pricesheets/read` não estiver disponível, o preço de varejo do Azure será exibido. Agora você pode usar a API de Preços de Varejo para obter preços de varejo

para todos os serviços do Azure. Anteriormente, a única maneira de recuperar preços para serviços do Azure era usar a Calculadora de Preços do Azure ou o portal do Azure. Para obter mais informações, consulte Visão geral dos preços de varejo do Azure.

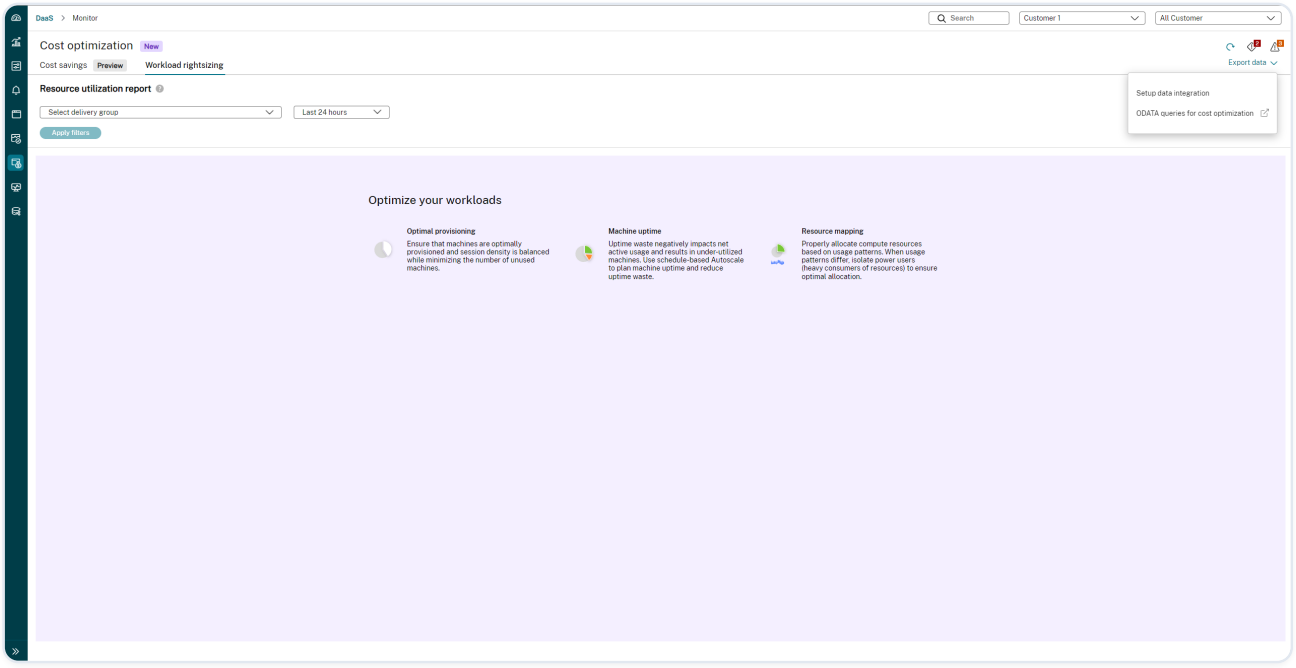
Calculando custos para máquinas que não sejam do Azure

Para outras máquinas, o custo é exibido com base no custo inserido pelos administradores no Web Studio. Se nenhum custo for mencionado no Web Studio, o custo padrão de $1 será considerado.

Exportar dados

Você pode exportar os dados na página **Otimização de custos** usando integração de dados e consultas ODATA. Para exportar dados, clique em **Exportar dados** na página **Otimização de custos**, as seguintes opções são exibidas:

- Configurar integração de dados
- Consultas ODATA para otimização de custos



Configurar integração de dados

Você pode integrar dados de otimização de custos com a API do Serviço Monitor, usando a qual você pode coletar os dados para solucionar e triar problemas. Para mais informações, consulte a página Integrações e exportações de dados.

Consultas ODATA para otimização de custos

Você pode usar as consultas ODATA de exemplo disponíveis na página de **Otimização de custos** para exportar dados.

Comece a usar o ODATA

Os links a seguir ajudam você a começar a usar o ODATA:

- Visão geral do ODATA
- Diferentes métodos para acessar dados do Serviço Monitor Citrix usando o endpoint OData v4 no Citrix Cloud
- Usar consultas de agregação OData V4 em dados do Serviço Monitor Citrix
- Como conectar o PowerBI ao DaaS Monitor usando OData e clientes de API
- Obter detalhes de usuários com alta duração de logon usando o Postman
- Como acessar os dados do Serviço Monitor
- Protocolo de Acesso a Dados

Exemplos de consultas ODATA

Descobrir VDA não utilizado

Para descobrir um VDA não utilizado, você deve fornecer um ID de grupo de desktop, data de início e data de término do VDA.

Para obter mais informações sobre como reduzir gastos com recursos não utilizados, consulte Dimensionamento de carga de trabalho.

Consulta de exemplo:

```
https://api-us.cloud.com/monitorodata/ResourceUtilizationSummary?
$apply=filter(DesktopGroupId eq desktop-group-id and granularity eq 1440
and SummaryDate ge startdate and SummaryDate lt enddate)/
groupby((MachineId), aggregate(cast(TotalSessionCount, Edm.Int32) with
average as AvgTotalSessionCount))/filter(AvgTotalSessionCount eq 0.0)/
aggregate($count as UnusedVDACount)
```

DESCOBRIR O TEMPO DE ATIVIDADE MÉDIO DIÁRIO EM MINUTOS

Para descobrir o tempo de atividade médio diário em minutos, você deve fornecer o seguinte:

- ID do grupo de desktop

- Data de início
- Data de término
- Diferença de dias entre a data de término e a data de início.

Para obter mais informações sobre como reduzir gastos com recursos não utilizados, consulte Dimensionamento de carga de trabalho.

Consulta de exemplo:

```
https://api-us.cloud.com/monitorodata/ResourceUtilizationSummary?
$apply=filter(desktopGroupId eq desktop-group-id and granularity eq 1440
and SummaryDate ge startdate and SummaryDate lt enddate)/
groupby((MachineId), aggregate(cast(UptimeInMinutes, Edm.Int32) div day-
difference with sum as TotalUptimeInMinutes))/
aggregate(TotalUptimeInMinutes with average as
DailyAverageUptimeInMinutes)
```

DESCOBRIR AÇÃO DE ENERGIA DE MÁQUINA COM FALHA

Para obter mais informações sobre a ação de energia de máquina com falha, consulte Ação de ligar com falha e Ação de desligar com falha.

Consulta de exemplo:

```
https://api-us.cloud.com/monitorodata/Machines?$filter=LifecycleState eq 0
and DesktopGroup/SessionSupport eq 1 and
(cast(LastPowerActionReason,'Edm.Int32') eq 6 or
cast(LastPowerActionReason,'Edm.Int32') eq 7 or
cast(LastPowerActionReason,'Edm.Int32') eq 8) and
(cast(LastPowerActionFailureReason,'Edm.Int32') eq 300 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 402 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 401) and MachineRole eq
0&$orderby=Name&$skip=0&$top=50&$expand=DesktopGroup($select=Name)&$select
=Sid,Id,Name,IsAssigned,IPAddress,FaultState,LastDeregisteredCode,FailureD
ate,CurrentPowerState,CurrentSessionCount,IsInMaintenanceMode,LastPowerAct
ionFailureReason,LastPowerActionCompletedDate
```

DESCOBRIR A ECONOMIA TOTAL

Para mais informações sobre economia de custos, consulte a página Economia de custos.

Exemplo de consulta:

```
https://api.cloud.com/monitorodata/MachineCostSavingsSummaries?
$apply=aggregate(TotalAmountSaved with sum as TotalAmountSavedSum)
```

DESCOBRIR O ESTADO DA MÁQUINA

Para mais informações sobre economia de custos, consulte a página Economia de custos.

Exemplo de consulta:

```
https://api.cloud.com/monitorodata/MachineCostSavingsSummaries?
$filter=SummaryDate eq
2024-08-09T06:00:00Z&$select=TotalMachinesCount,PowerManagedMachinesOff,Po
werManagedMachinesInHibernate,PowerManagedMachinesOnWithSessions,PowerMana
gedMachinesOnWithoutSessions
```

Economia de custos

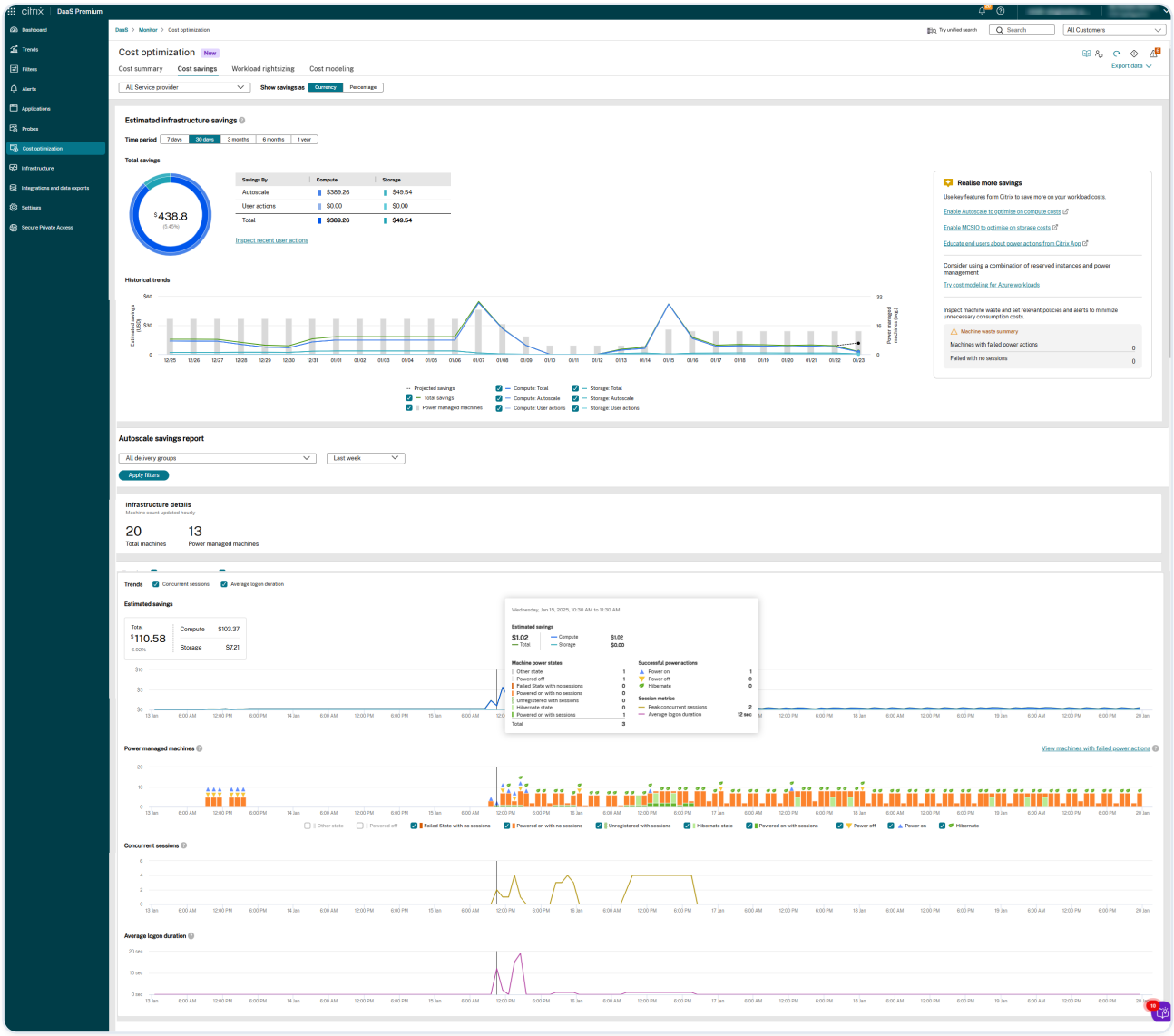
A página Economia de custos fornece uma representação visual da economia de infraestrutura acumulada durante um período selecionado e prevê a economia esperada para os dias restantes. Ao analisar o uso e as sessões das máquinas, esta página ajuda a identificar a economia alcançada e as oportunidades de redução de custos. Esta página oferece:

- Visão sobre a otimização dos custos de infraestrutura
- O valor economizado
- Informações sobre uma série de cenários que podem resultar na superação dos custos projetados
- Oportunidades potenciais para identificação e planejamento estratégico para realizar economia de custos de infraestrutura

O uso da máquina geralmente aumenta durante os horários de pico, exigindo mais recursos. O recurso Autoscale™ ajuda a reduzir custos desligando automaticamente as máquinas não utilizadas durante o período de baixa demanda. A economia projetada depende desse padrão de uso. No entanto, os custos podem exceder as expectativas em circunstâncias específicas, como quando há máquinas não utilizadas ou quando há falhas nas ações de energia do Autoscale. Identificar as razões por trás dessas ocorrências era anteriormente um desafio.

A página **Otimização de Custos** fornece informações detalhadas sobre diferentes cenários que podem fazer com que você exceda o custo esperado. Por exemplo, se houver máquinas sem sessões, ela mostra mais oportunidades de economia de custos.

Clique na guia **Otimização de Custos** no menu esquerdo da página **Início** para acessar a página **Otimização de Custos**.



Na lista suspensa na parte superior, se um site tiver provedores de nuvem e locais, agora você pode filtrar por todos os provedores de nuvem, todos os provedores locais ou provedores individuais.

Nota:

> O filtro é aplicado imediatamente após a seleção, sem um botão de aplicar.

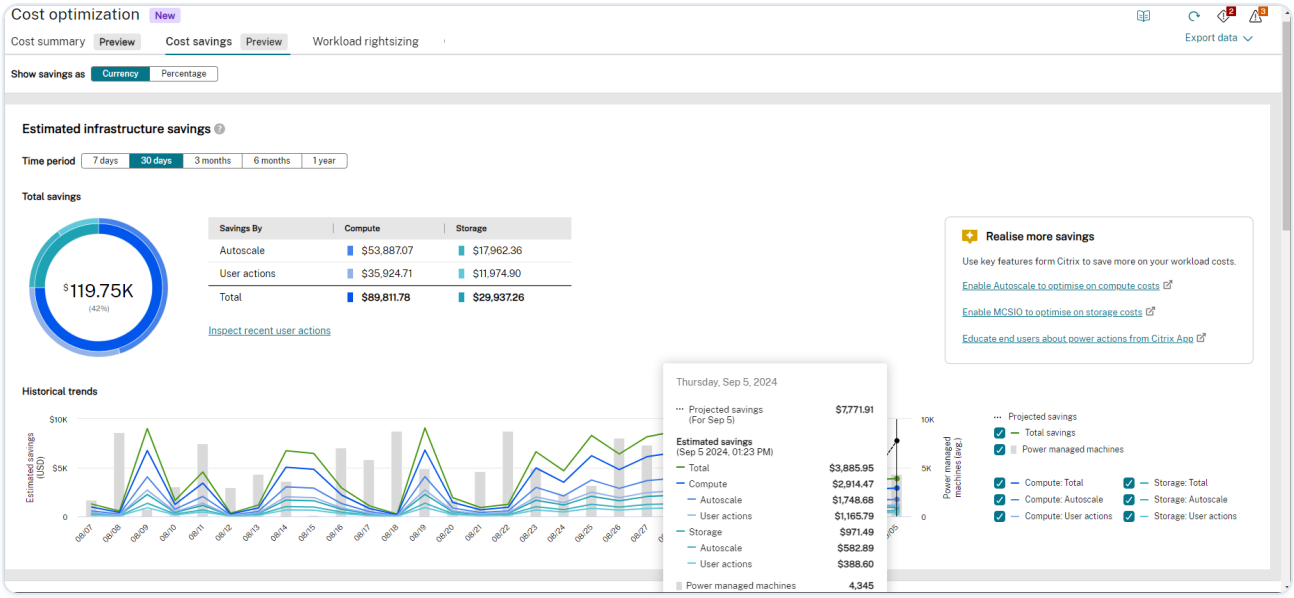
> A página **Otimização de Custos** exibe **Economia de infraestrutura estimada** e **Relatório de economia do Autoscale**. Você pode visualizar a economia de custos na moeda do hipervisor ou como uma porcentagem do custo incorrido.

Economia de Infraestrutura Estimada: Esta representação gráfica ajuda a avaliar a utilização eficiente dos recursos de infraestrutura. Este gráfico mostra a economia alcançada a partir da economia relacionada à computação e da economia de armazenamento.

> **Nota:**
>
> Para visualizar as economias de armazenamento:
>
> - O Autoscale deve estar habilitado para otimizar os custos de computação. Para obter mais informações, consulte Introdução ao Autoscale.
> - Altere o tipo de armazenamento para um nível inferior quando uma VM for desligada para otimizar os custos de armazenamento. Para obter mais informações, consulte a documentação Alterar o tipo de armazenamento para um nível inferior quando uma VM é desligada.
> - Este recurso é atualmente aplicável apenas a máquinas Azure.
>
> Você pode visualizar os resultados para os últimos:

- Sete dias
- Trinta dias
- Três meses
- Seis meses
- Doze meses

A imagem a seguir mostra a seção **Economias de infraestrutura estimadas**:



A tabela a seguir lista os elementos do gráfico de Economias estimadas:

ELEMENTO	DESCRIÇÃO
Economia total	Exibe a economia total alcançada na infraestrutura para a duração selecionada. A economia é ainda categorizada em custos de armazenamento e computação e está disponível em formato tabular.
Economia estimada	Exibe o valor da economia alcançada na infraestrutura para a duração selecionada.
Máquinas com gerenciamento de energia	Exibe o número total de máquinas com gerenciamento de energia.
Economia projetada	Exibe quanta economia de infraestrutura pode ser feita para a duração restante.
Computação - Total	Exibe a economia total alcançada a partir da economia relacionada à computação.
Computação - Autoescala	Exibe a economia total alcançada a partir da economia relacionada à computação que utiliza o recurso de autoescala.
Computação - Ações do usuário	Exibe a economia total alcançada a partir da economia relacionada à computação que são provenientes de ações do usuário.

ELEMENTO	DESCRIÇÃO
Armazenamento - Total	Exibe a economia total obtida com a economia de armazenamento.
Armazenamento - Autoscale	Exibe a economia total obtida com a economia de armazenamento que está usando o recurso de autoscale.
Armazenamento - Ação do usuário	Exibe a economia total obtida com a economia de armazenamento que são de ações do usuário.

Relatório de Economia do Autoscale: Esta representação gráfica fornece o relatório de economia para os grupos de entrega para os quais o recurso Autoscale está configurado e habilitado. Este relatório é aplicável apenas para máquinas com gerenciamento de energia. Você pode selecionar um grupo de entrega e, em seguida, selecionar dados para hoje, ontem, semana passada, próxima semana, este mês ou próximo mês. Você pode passar o mouse sobre qualquer gráfico para recuperar valores específicos do gráfico.

> **Nota:**

> Se o grupo de entrega for excluído, você não poderá obter nenhum dado no relatório de economia do Autoscale.

> Você pode detalhar as seguintes opções na lista suspensa de grupos de entrega:

- **Todos os grupos de entrega**: Os detalhes da infraestrutura exibem todas as informações do grupo de entrega.
- **Todas as sessões únicas**: Detalhes da infraestrutura para todos os grupos de entrega que são máquinas de sessão única, juntamente com a representação gráfica do estado de energia da máquina, ações de energia bem-sucedidas do Autoscale e sessões ao passar o mouse sobre o gráfico.
- **Todas as sessões múltiplas**: Detalhes da infraestrutura para todos os grupos de entrega que são máquinas de sessão múltipla, juntamente com a representação gráfica.
- **Selecionar até 15** - Os detalhes da infraestrutura exibem todos os grupos de entrega selecionados, até 15, juntamente com uma representação gráfica.

- **Excluir até 15** - Os detalhes da infraestrutura exibem todos os grupos de entrega, excluindo os grupos de entrega selecionados, até 15, com uma representação gráfica.

Os dados são exibidos para a duração selecionada. A representação gráfica das **Economias estimadas** são as economias reais da seleção feita no menu suspenso. Ao passar o mouse sobre os pontos de pico, são exibidas informações sobre o estado de energia da máquina, ações de energia bem-sucedidas do Autoscale e sessões.

Com base no grupo de entrega selecionado, você pode visualizar os seguintes detalhes:

- **Detalhes da infraestrutura**
  - Total de máquinas e máquinas gerenciadas por energia - Exibe o número total de máquinas e, destas, quantas são gerenciadas por energia. Esses dados oferecem uma oportunidade adicional para considerar a conversão das máquinas restantes não gerenciadas por energia em máquinas gerenciadas por energia, habilitando assim o recurso Autoscale para uma cobertura mais abrangente. Os dados na seção Detalhes da infraestrutura mostram as últimas informações conhecidas, atualizadas a cada hora.
- **Detalhes do catálogo**

  Exibe o nome dos hipervisores (provedores de serviço). Para obter mais informações, consulte Plataformas de hospedagem VDA compatíveis. Os dados nos Detalhes do catálogo mostram os dados mais recentes (dados em tempo real) disponíveis no momento atual.

  Você pode obter os seguintes detalhes:

  - **Nome do hipervisor** - Exibe o nome do hipervisor ao qual o site está conectado. Exibe todos os hipervisores disponíveis quando vários hipervisores estão presentes.
  - **Instância** - Exibe o nome da instância.
  - **Custo total por hora** - Exibe o custo por máquina por hora na moeda que o hipervisor suporta. Para máquinas Azure, quando a permissão Microsoft.Consumption/pricesheets/read está disponível, o preço efetivo é exibido na moeda configurada na assinatura do Azure. Se as permissões não estiverem disponíveis, o preço de varejo do Azure será exibido. Para obter mais informações, consulte Visão geral dos preços de varejo do Azure. Para outras máquinas, o custo é exibido com base no custo inserido pelos administradores no Web Studio. O custo padrão é de US$ 1 se o custo não for mencionado no Web Studio. Para obter mais informações, consulte Como o custo é calculado para otimizar o custo?.
  - **Custo de computação por hora** - Exibe a economia de custos proveniente das economias relacionadas à computação.

  - **Custo de armazenamento por hora** - Exibe a economia de custos proveniente das economias de armazenamento.
  - **Máquinas** - Exibe a contagem de máquinas para a instância selecionada.

- **Configuração do Autoscale (última conhecida)**

  Tag em uso - Exibe a tag das máquinas configuradas nas configurações do Autoscale em um WebStudio. Você também pode filtrar os dados com base nas máquinas marcadas. Neste caso, você obtém apenas o resumo das máquinas marcadas.

  Buffer de capacidade (pico) e **Buffer de capacidade (fora de pico)**

  Exibe a porcentagem de buffer para máquinas ligadas com base no requisito máximo do grupo de entrega durante os horários de pico e fora de pico.

- **Economia estimada**

  Exibe o valor da economia alcançada na infraestrutura para a duração selecionada. Você pode visualizar a economia proveniente de economias relacionadas à computação e economias relacionadas ao armazenamento para as máquinas Azure com o recurso Autoscale ativado.

- **Máquinas com gerenciamento de energia**

  Com o Autoscale ativado, as máquinas com gerenciamento de energia são desligadas quando não estão em uso para otimizar custos. Você pode obter os seguintes detalhes:

  - Número de máquinas desligadas - Esses dados ajudam você a analisar o número de máquinas que foram desligadas e, assim, ajudaram a reduzir custos.
  - Estado de hibernação - Esses dados ajudam você a analisar quantas máquinas estão no estado de hibernação.
  - Máquinas ligadas sem sessões - Esses dados oferecem a oportunidade de analisar por que as máquinas estavam ativas sem sessões e de planejar uma estratégia de economia de infraestrutura mais eficaz.
  - Máquinas ligadas com sessões - Esses dados ajudam você a analisar o número de máquinas que foram ligadas e com sessões ativas.
  - Desligar - Esses dados ajudam você a analisar o número de máquinas que foram desligadas ou suspensas e quando essa ação foi realizada. Você pode verificar esses dados e fazer modificações adicionais, contribuindo para a redução de custos.

- Ligar - Esses dados ajudam você a analisar quantas máquinas foram ligadas e quando essa ação foi realizada. Você pode verificar esses dados e fazer modificações adicionais e, assim, ajudar a reduzir custos.
- Estado de falha sem sessões: Este campo exibe a contagem de máquinas que estão em um estado de falha e não têm sessões ativas.
- Não registradas com sessões: Este campo exibe a contagem de máquinas que estão em um estado não registrado mas ainda estão atendendo sessões.

> **Observação:**
>
> Você pode ver a contagem de máquinas no estado Falha sem sessões e Máquinas com ações de energia falhas e tomar ações com base no motivo da falha, tempo e grupo de entrega. As contagens são links clicáveis que navegar para a página Filtros para ações adicionais. A contagem inclui máquinas de sessão única e de múltiplas sessões.

- **Sessões simultâneas**

  Exibe o número total de sessões no horário selecionado. Esses dados ajudam você a determinar quando desligar máquinas para otimização de custos.

- **Duração média do logon**

  Exibe o tempo médio para um usuário fazer logon durante a duração de tempo selecionada.

Dimensionamento de carga de trabalho

A página aprimorada de dimensionamento de carga de trabalho ajuda você a analisar os aspectos de uso e dimensionamento dos seus grupos de entrega. Assim, os grupos de entrega podem ser analisados com base na atividade da máquina ou do usuário.

A análise baseada em máquina permite que você:

- Categorize desktops virtuais com base no uso para identificar máquinas com nenhuma ou baixa atividade e reduzir gastos com recursos não utilizados.Análise de Uso
- Analise a utilização de recursos em desktops virtuais para identificar máquinas que precisam ser dimensionadas corretamente para reduzir custos ou melhorar a experiência do usuário.Análise de Dimensionamento

A análise baseada no usuário permite que você:

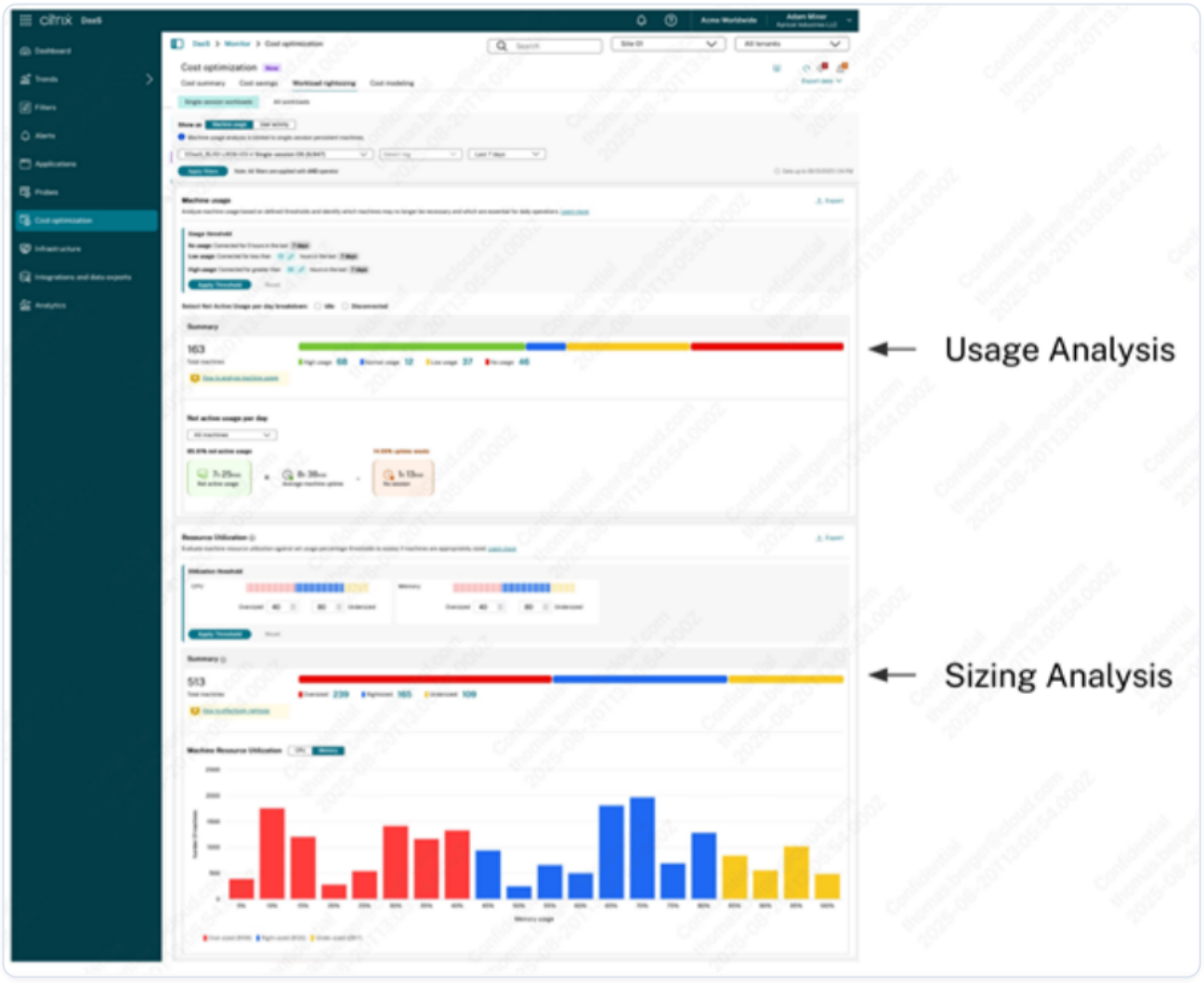
- Categorize os usuários com base em sua atividade. Considere remover o direito de acesso de usuários sem atividade por motivos de higiene de TI. Usuários com baixo uso podem ser movidos para recursos compartilhados para um uso mais eficiente dos recursos.
- Analise o consumo de recursos dos usuários para identificar grupos com consumo de recursos acima ou abaixo da média, e para distribuir os usuários de forma mais eficaz.

Clique na guia **Otimização de Custos** no menu esquerdo da página inicial. E então, clique na guia **Dimensionamento de carga de trabalho** para acessar a página **Dimensionamento de carga de trabalho**.

> **Observação:**

> Na parte superior da página, você pode alternar entre a análise baseada em máquina e a análise baseada em usuário.

> Você também pode clicar no link **Dimensionar este grupo de entrega** na seção **Detalhes da infraestrutura** na **guia Otimização de Custos > Economia de custos** para acessar a página **Dimensionamento de carga de trabalho**.



A análise de máquina é ideal para cenários com desktops virtuais atribuídos estaticamente aos usuários, como Windows 365 Enterprise ou Frontline dedicado. A análise de usuário é útil para a análise de grupos de entrega com desktops virtuais atribuídos aleatoriamente. Ambas as análises estão atualmente limitadas a máquinas de sessão única.

> **Observação:**

> A análise clássica de dimensionamento correto, acessível através do botão “Todas as Cargas de Trabalho” na parte superior da página, será descontinuada em uma próxima versão.

Análise de uso

A análise de uso permite categorizar desktops virtuais com base em seus níveis de atividade da seguinte forma:

- **Máquinas de baixo ou nenhum uso (Máquinas dedicadas)**: As máquinas nesta categoria podem não ser mais necessárias e podem ser removidas para economizar custos.
- **Máquinas de alto uso (Máquinas dedicadas)**: Esta categoria é crítica para as operações diárias e pode exigir medidas adicionais de continuidade de serviço.
- **Usuários de baixo ou nenhum uso (Máquinas agrupadas)**: Usuários sem atividade dentro do período selecionado podem não precisar mais ser atribuídos ao grupo de entrega. Removê-los pode ajudar a reduzir os custos do seu ambiente. Usuários com baixa atividade podem se beneficiar de uma reatribuição. Para consolidar o uso e reduzir custos, considere mover usuários com baixa atividade que possuem um desktop dedicado para um desktop agrupado.

Para realizar a análise de uso:

1. Selecione máquinas com base em Grupos de Entrega ou Tags
2. Escolha o período para análise.
3. Revise e configure os limites que definem padrões de uso baixo e alto.
4. Examine a seção de resumo que mostra a categorização do desktop virtual com base nos limites configurados.
5. Revise a seção de uso ativo líquido que exibe os detalhes de uso para cada máquina. O tempo ocioso e desconectado pode ser incluído ou excluído na análise de uso ativo líquido.
6. Use o menu suspenso para focar em categorias específicas.
7. Exporte nomes de máquinas e usuários associados usando a função de exportação para revisar os nomes das máquinas e seus usuários associados.

> **Nota:**
>
> O exemplo fornecido ilustra a análise de uso baseada em máquina; no entanto, as etapas para análise baseada em usuário são equivalentes e não são discutidas separadamente.



Análise de dimensionamento

A análise de dimensionamento categoriza desktops virtuais ou usuários com base na utilização de recursos da seguinte forma:

- Máquinas superdimensionadas: Têm mais recursos do que o necessário; a redução da alocação de recursos pode diminuir os custos sem impactar a experiência do usuário
- Máquinas subdimensionadas: Não têm recursos suficientes; a experiência do usuário pode ser melhorada alocando mais recursos
- Máquinas com dimensionamento correto: Ficam entre os limites de superdimensionamento e subdimensionamento
- Usuários leves: Esses usuários podem se beneficiar da reatribuição. Para consolidar e reduzir custos, considere mover usuários leves com um desktop dedicado para um desktop compartilhado em pool.
- Usuários moderados: Usuários moderados são atribuídos corretamente a máquinas em um grupo de entrega e devem esperar uma experiência de usuário ideal.
- Usuários avançados: Usuários avançados consomem recursos significativos e, quando compartilham um desktop em pool, seu alto uso pode impactar negativamente a experiência geral para outros usuários nessa máquina. Para aprimorar a experiência de todos os usuários e garantir que os usuários avançados tenham acesso consistente a um desktop, considere mover esses usuários para um desktop dedicado ou atribuí-los a grupos de entrega individuais.

Para realizar a Análise de Dimensionamento:

1. Selecione máquinas com base em Grupos de Entrega ou Tags
2. Escolha o período para análise.
3. Configure limites separados para a utilização de CPU e Memória.
4. Revise a seção de resumo mostrando a categorização do desktop virtual
5. Analise o gráfico de utilização de recursos da máquina mostrando a distribuição de CPU e Memória
6. Ajuste fino das configurações da máquina com base no tipo de recurso e identifique anomalias
7. Exporte os nomes das máquinas e usuários associados usando a função de exportação para revisar os nomes das máquinas e seus usuários associados

Observação:

O exemplo fornecido ilustra a análise de consumo de recursos baseada em máquina; no entanto, as etapas para a análise baseada em usuário são equivalentes e não são discutidas separadamente.



> **Observação:**

> A análise de utilização usa a utilização do percentil 95 para grupos de entrega no período selecionado, indicando que 95% da utilização de CPU ou Memória está no valor definido ou abaixo dele.

Melhores práticas

- Use a análise de uso para identificar oportunidades de economia de custos removendo máquinas subutilizadas.
- Aplique a análise de dimensionamento para otimizar a alocação de recursos e melhorar a experiência do usuário.
- Use a análise de máquina para cenários de desktop virtual atribuídos estaticamente para uma análise precisa.
- Use a atividade do usuário para cenários de desktop virtual agrupados para uma análise precisa.
- Considere os padrões de roaming ao analisar desktops virtuais atribuídos aleatoriamente.
- Exporte relatórios detalhados para análise e documentação adicionais.

Principais termos e gráficos

Uso ativo líquido da máquina: O uso ativo líquido é calculado deduzindo o desperdício total de tempo de atividade do tempo de atividade médio da máquina. Todos os tempos estão em minutos.

Porcentagem de Uso Ativo Líquido: O tempo real em que os usuários usaram ativamente a máquina. Esta é a duração em que pelo menos uma sessão estava ativa enquanto a máquina estava ligada.

Tempo de Atividade Médio da Máquina: O tempo total em que a máquina esteve ligada.

Sem Sessão: O tempo de atividade desperdiçado devido à ausência de sessões ativas.

Tempo Ocioso: Tempo de atividade desperdiçado devido a sessões ociosas. Este é o tempo em que todas as sessões na máquina estão ociosas.

Tempo Desconectado: Tempo de atividade desperdiçado devido a sessões desconectadas. Este é o tempo em que todas as sessões na máquina estão desconectadas.

Total de máquinas - Exibe o número total de máquinas. Isso inclui todas as máquinas que foram ligadas durante o período selecionado.

Densidade média de sessão - Esta é uma média entre o número de máquinas e o período de tempo selecionado. Refere-se à quantidade de carga de sessão em uma máquina que afeta o recurso disponível para as sessões.

Máquinas não utilizadas - Exibe o número de máquinas que não tiveram sessões durante o período selecionado, mas que ainda estavam ligadas.

Utilização da CPU:

Coorte de máquinas - Fornece informações sobre os grupos de máquinas categorizados em superior, médio e inferior com base na sua utilização da CPU. O limite dos limiares pode ser configurado pelos administradores.

Intervalo de Picos de CPU - Exibe o intervalo dos picos de CPU com base na sua utilização correspondente à coorte de máquinas.

Máquinas - Exibe o número de máquinas correspondente à coorte de máquinas.

Densidade de sessão - Exibe a densidade de sessão correspondente à coorte de máquinas.

Tendências de utilização de recursos:

Intervalo de picos de CPU - Exibe o intervalo de picos de CPU em uma faixa. Ao passar o mouse sobre qualquer ponto na faixa, o valor superior e inferior da faixa é exibido.

Utilização máxima de memória - Exibe a maior utilização de memória para as máquinas selecionadas e para o tempo selecionado em um gráfico.

Densidade média de sessão - Exibe a densidade média de sessão para as máquinas selecionadas e para o tempo selecionado em um gráfico.

RTT ICA médio - Exibe o tempo médio de ida e volta para a sessão. Este gráfico mostra interrupções quando não há sessões ativas ou quando as sessões são desconectadas.

Duração média de logon - Exibe a duração média de logon para as máquinas selecionadas e para o período de tempo selecionado em um gráfico. Este gráfico mostra dados quando um novo logon é iniciado durante o tempo selecionado.

Resumo de custos

A página **Resumo de custos** fornece um resumo abrangente das despesas associadas à execução do ambiente Citrix®. Com esta melhoria, você obtém visibilidade sobre:

- O custo total por usuário
- Custo de entrega de virtualização pelos provedores de carga de trabalho escolhidos, tipos de desktop e conjuntos de séries de VM

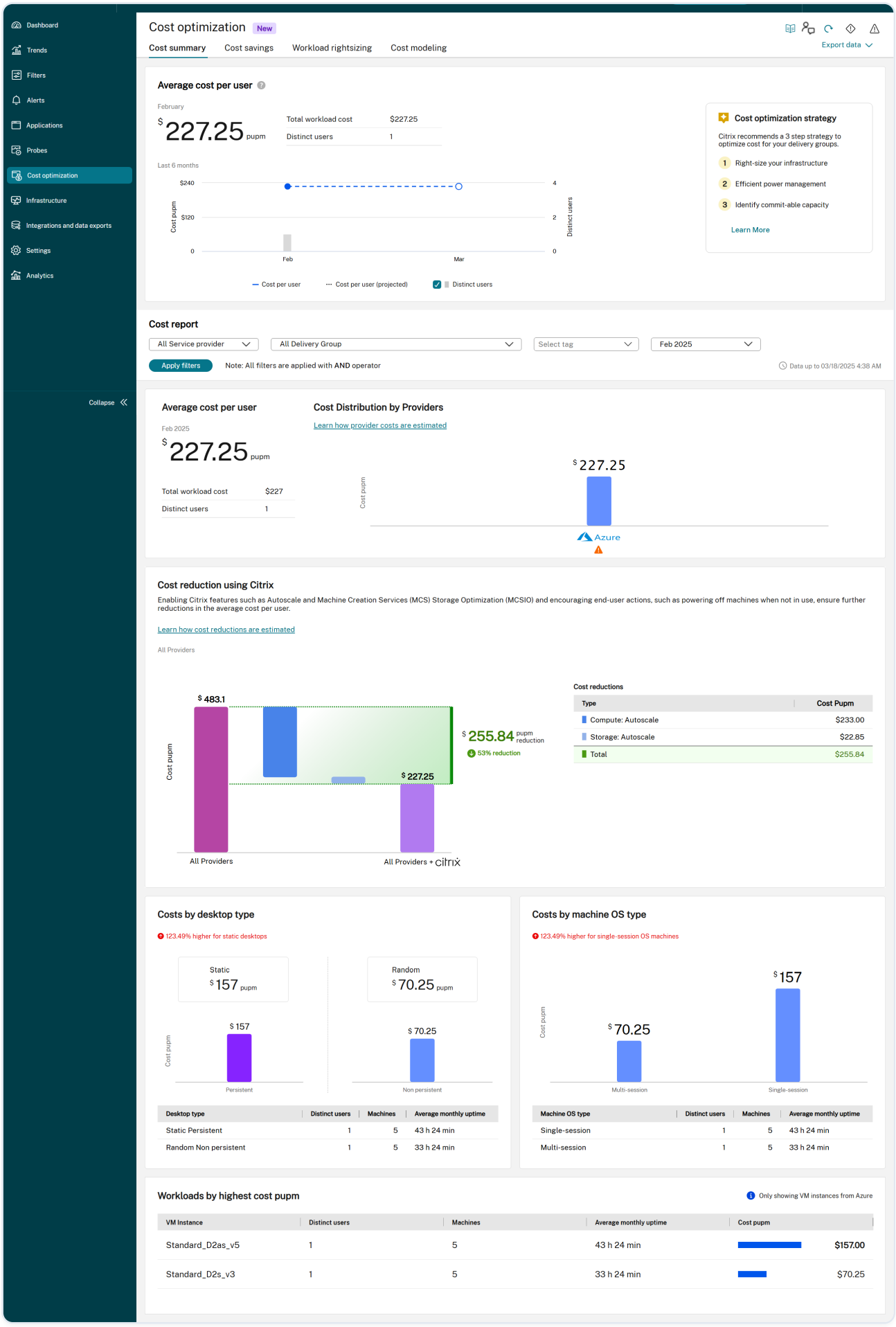
Esta página oferece:

- Visão sobre o custo de entrega de um aplicativo ou desktop virtualizado a um usuário
- O valor economizado
- Informações sobre custos e economias categorizadas por:
  - Provedor de plataforma
  - Tipo de SO
  - Tipo de desktop
  - Série de VM

> **Nota:**

> A página **Resumo de custos** está disponível somente se o site estiver em execução por pelo menos 15 dias em um mês.

> Para acessar a página **Resumo de custos**, clique em **Monitorar** > **Otimização de custos** > **Resumo de custos**. A página **Resumo de custos** aparece:


Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Cost optimization
New
Cost summary
Cost savings
Workload rightsizing
Cost modeling
Export data
Average cost per user
February
$ 227.25 pupm
Total workload cost $227.25
Distinct users 1
Last 6 months
$240
$120
0
Cost pupm
4
2
0
Distinct users
Feb
Mar
Cost per user
Cost per user (projected)
Distinct users
Cost optimization strategy
Citrix recommends a 3 step strategy to optimize cost for your delivery groups.
1 Right-size your infrastructure
2 Efficient power management
3 Identify commit-able capacity
Learn More
Cost report
All Service provider
All Delivery Group
Select tag
Feb 2025
Apply filters
Note: All filters are applied with AND operator
Data up to 03/18/2025 4:38 AM
Average cost per user
Feb 2025
$ 227.25 pupm
Total workload cost $227
Distinct users 1
Cost Distribution by Providers
Learn how provider costs are estimated
$ 227.25
Cost pupm
Azure
Cost reduction using Citrix
Enabling Citrix features such as Autoscale and Machine Creation Services (MCS) Storage Optimization (MCSIO) and encouraging end-user actions, such as powering off machines when not in use, ensure further reductions in the average cost per user.
Learn how cost reductions are estimated
All Providers
$ 483.1
Cost pupm
$ 227.25
All Providers
All Providers + citrix
$ 255.84 pupm reduction
53% reduction
Cost reductions
Type
Cost Pupm
Compute: Autoscale $233.00
Storage: Autoscale $22.85
Total $255.84
Costs by desktop type
123.49% higher for static desktops
Static
$ 157 pupm
Random
$ 70.25 pupm
$ 157
$ 70.25
Cost pupm
Persistent
Non persistent
Desktop type
Distinct users
Machines
Average monthly uptime
Static Persistent 1 5 43 h 24 min
Random Non persistent 1 5 33 h 24 min
Costs by machine OS type
123.49% higher for single-session OS machines
$ 157
$ 70.25
Cost pupm
Multi-session
Single-session
Machine OS type
Distinct users
Machines
Average monthly uptime
Single-session 1 5 43 h 24 min
Multi-session 1 5 33 h 24 min
Workloads by highest cost pupm
Only showing VM instances from Azure
VM Instance
Distinct users
Machines
Average monthly uptime
Cost pupm
Standard_D2as_v5 1 5 43 h 24 min $157.00
Standard_D2s_v3 1 5 33 h 24 min $70.25

A página **Resumo de custos** inclui:

- **Custo médio por usuário**

  Você pode visualizar o custo real por usuário por mês nos últimos seis meses e também o custo projetado para o mês atual. Além disso, você pode ver o custo total das cargas de trabalho e o número de usuários distintos no site. Quando várias moedas estão envolvidas, os custos são exibidos em USD se o USD for uma delas. Caso contrário, o custo é exibido em uma moeda selecionada aleatoriamente da lista. A economia de custos em comparação com o mês anterior e o penúltimo mês é fornecida em porcentagem. Além disso, as alterações no número de usuários distintos também são apresentadas. A representação gráfica mostra a tendência para cada mês.

  Você pode usar o custo médio por usuário e otimizar o uso.

- **Relatório de custos**

  Você pode visualizar o relatório de custos dos provedores de serviços selecionados, para o grupo de entrega selecionado e para a tag selecionada. Você pode visualizar o relatório dos últimos três meses separadamente ou uma visão consolidada dos dados dos últimos três meses.

- **Redução de custos usando o Citrix**

  Você pode reduzir ainda mais o custo médio por usuário ativando recursos do Citrix, como Autoscale e Machine Creation Services™ (MCS), Otimização de Armazenamento (MCSIO). Além disso, incentive ações do usuário final, como desligar máquinas quando não estiverem em uso.

  Esses dados exibem a economia total quando os recursos do Citrix são aplicados. Também exibe a economia proveniente das ações do usuário final.

- **Custo por tipo de desktop**

  Você pode visualizar os custos dos seguintes tipos de desktops:

  - **Estático persistente:** O usuário faz logon no mesmo desktop virtual todas as vezes e as alterações feitas no desktop são salvas.
  - **Estático não persistente:** O usuário faz logon no mesmo desktop virtual todas as vezes e as alterações feitas no desktop não são salvas.
  - **Aleatório persistente:** O usuário recebe um desktop virtual do pool de desktops e as alterações feitas no desktop são salvas.

    - **Não persistente aleatório:** O usuário recebe um desktop virtual do pool de desktops e as alterações feitas no desktop não são salvas.

  Você pode visualizar o número de usuários distintos, máquinas e o tempo de atividade mensal médio para cada tipo de máquina.

  Você pode usar esses dados e planejar a economia de custos movendo usuários para diferentes tipos de desktops. Por exemplo, tipos de desktop persistentes estáticos exigem mais uso de recursos em comparação com desktops não persistentes aleatórios. Assim, você pode planejar mover alguns usuários de tipos de desktop persistentes estáticos para tipos de desktop não persistentes aleatórios.

- **Custo por tipo de SO**

  Você pode visualizar os custos de tipos de SO de sessão única e multi-sessão. Você pode visualizar o tipo de SO da máquina, usuários distintos, máquinas e o tempo de atividade mensal médio. Você pode usar esses dados e planejar a economia de custos movendo usuários para diferentes tipos de SO.

- **Cargas de trabalho por maior custo por usuário por mês**

  Você pode visualizar os detalhes do maior custo por usuário por mês, incluindo a instância da máquina virtual, o número de usuários distintos e o tempo de atividade médio da máquina. Além disso, você pode ver o número de máquinas e o custo por usuário.

  Use esses dados para visualizar o custo de cada tipo de configuração de VM e decidir quais configurações atribuir aos usuários.

Modelagem de custos

O novo recurso de modelagem de custos suporta cargas de trabalho do Azure e fornece recomendações com base em padrões de uso. Os clientes recebem recomendações sobre se as Reservas do Azure ou o Plano de Economia são mais adequados para proporcionar a máxima economia de custos. Os clientes de Reservas do Azure reservam um número específico de máquinas antecipadamente a um custo fixo com desconto, enquanto os planos de economia permitem que eles se comprometam com um valor em dólar para taxas com desconto. O recurso analisa os últimos 28 dias de dados para fornecer recomendações estimadas. Isso ajuda os clientes a economizar custos tomando decisões informadas sobre a alocação de recursos.

> **Observação:**

- Para estimativas ideais, recomenda-se usar dados de um ambiente estável nos últimos 28 dias. Evite usar dados de períodos de atividade incomum, como férias ou picos repentinos de uso. Espere até que seu uso retorne aos níveis de base antes de seguir essas recomendações.
- A modelagem de custos é projetada para cargas de trabalho baseadas em nuvem com preços flexíveis. Para cargas de trabalho com preços mensais fixos ou para cargas de trabalho locais, use Dimensionamento de Carga de Trabalho em vez disso.

Benefícios:

- Fornece recomendações personalizadas para economia de custos.
- Suporta planos de reserva e de economia.
- Analisa dados de uso recentes para insights precisos.
- Ajuda a otimizar a alocação de recursos e reduzir despesas.
- Oferece flexibilidade na seleção de grupos de entrega, tags, séries de VM e regiões.

Observação:

A modelagem de custos é suportada apenas para cargas de trabalho do Azure.

Tipos de planos

No Azure, existem dois tipos de planos para economizar custos:

- **Azure Reservations**: Os clientes decidem quantas máquinas reservar antecipadamente. A reserva tem um custo fixo diferente com uma taxa de desconto em comparação com o custo pago conforme o uso.
- **Savings Plan**: Os clientes se comprometem com um valor específico em dólares, em vez de um número de máquinas. Até que esse valor seja consumido, eles são cobrados com um custo com desconto. Depois disso, eles pagam o custo pago conforme o uso.

A página de **Modelagem de custos** fornece recomendações para cada plano de forma independente, mostrando economias potenciais.

Clique em **Otimização de custos > Modelagem de custos**. A página **Modelo de custos e cargas de trabalho na nuvem** é exibida.

CITRIX DAAS™

citrix | DaaS Premium | 0 - Production

DaaS > Monitor > Cost optimization

Try unified search | Search | 1 - Production

Cost optimization New

Cost summary | Cost savings | Workload rightsizing | Cost modeling

Export data

Cost model cloud workloads

We recommend that you filter only by long-term-use machines and production workloads. Delivery groups and machines used for testing or short-term use may skew the cost model results.

All delivery groups | Select tag | All VM series | All regions

Apply filters | Note: All filters are applied with **AND** operator

Data up to 04/03/2025 9:56 AM | Download report

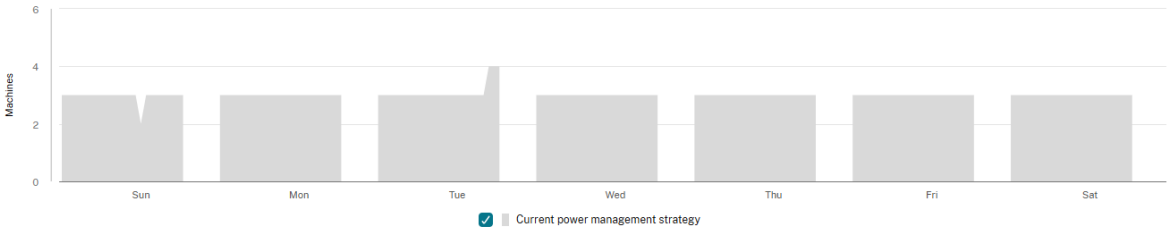
Cost model based on power management strategy

Choose from various Autoscale power management strategies to visualize concurrent machine consumption and savings opportunities.

No changes to Autoscale	Potential changes to Autoscale	
Current power management strategy Analyze potential savings opportunities by utilizing the existing Autoscale configuration.	**Deallocate machines at session end** Analyze potential savings opportunities if Autoscale is configured to deallocate machines at the end of a user's session. **95.45% reduced machine consumption**	**Deallocate machines for inactive session** Analyze potential savings opportunities if Autoscale is configured to deallocate machines when a session is inactive. **99.01% reduced machine consumption**

Concurrent machine consumption

Concurrent machine consumption is analyzed based on the last 28 days of historical consumption.



Savings opportunity

Determine the best commitment strategy and term length based on the selected power management strategy. View cost analysis

	Reserved instances		Savings plan	
	1 year	3 year	1 year	3 year
Potential savings opportunity	**40 %** Save up to $2,717.07 / yr	**61 %** Save up to $4,142.95 / yr	**31 %** Save up to $2,074.39 / yr	**53 %** Save up to $3,570.76 / yr
Commitment	$3,978.07 / yr	$2,552.20 / yr	$4,620.75 / yr	$3,124.39 / yr
Pay as you go	$72.58 / yr	$72.58 / yr	$72.58 / yr	$72.58 / yr
Total	**$4,050.65 / yr**	**$2,624.78 / yr**	**$4,693.33 / yr**	**$3,196.97 / yr**

Recommendations

Review the recommended changes to your commitment strategy based on the term length.

			Machines to be reserved		Savings plan hourly commitment (USD)	
Virtual machine series	Region	Current machines	1 year	3 year	1 year	3 year
Standard_D4s_v3	eastus	727	2	2	$0.26 / hr	$0.18 / hr
Standard_D8as_v4	eastus	21	1	1	$0.26 / hr	$0.18 / hr

Analyze per virtual machine series

Validate the optimum number of machines required per series by correlating with respective cost per user.

Virtual machine series

Standard_D4s_v3 in eastus

Export analysis



Você pode selecionar todos os grupos de entrega, até 15 (ou a contagem real) grupos de entrega, e excluir até 15 (ou a contagem real) grupos de entrega, se necessário. Você pode selecionar **Todas as sessões únicas** ou **Todas as sessões múltiplas** nas listas suspensas. Você também pode filtrar por **Tags**, **Série de VMs** e **Regiões**. Se você não selecionar nenhuma opção, a análise será executada no conjunto de dados aplicável completo por padrão, considerando os últimos 28 dias de dados.

> **Nota:**
>
> A recomendação de modelagem de custos é baseada em dados dos últimos 28 dias e assume que o comportamento durante este período permanece consistente.

Estratégias de gerenciamento de energia

A análise de dados varia com base na estratégia de gerenciamento de energia selecionada. Você pode selecionar uma das seguintes estratégias de gerenciamento de energia Autoscale™ para visualizar o consumo simultâneo de máquinas e as oportunidades de economia:

- **Estratégia de gerenciamento de energia atual**: Selecione esta estratégia para analisar economias potenciais usando a configuração Autoscale existente. Não há alteração na configuração Autoscale. A modelagem de custos recomendada é gerada com base na configuração Autoscale atual, calculando os custos para todas as máquinas que estão ativas e em execução.
- **Desalocar máquinas no final da sessão**: Selecione esta estratégia se você estiver disposto a alterar a configuração Autoscale para desalocar máquinas no final das sessões do usuário para analisar economias potenciais. A modelagem de custos recomendada é gerada com base na configuração Autoscale atualizada, calculando os custos apenas para o tempo de sessão ativa, ignorando o tempo de desconexão.
- **Desalocar máquinas para sessão inativa**: Selecione esta estratégia se você estiver disposto a alterar a configuração Autoscale para desalocar máquinas quando as sessões estiverem inativas para analisar economias potenciais. A modelagem de custos recomendada é gerada com base na configuração Autoscale atualizada, calculando os custos apenas para o tempo em que as sessões estão ativas e não ociosas.

Por exemplo, se a máquina estiver ativa por 60 minutos e a sessão for desconectada por 20 minutos, os 40 minutos restantes são o tempo de sessão ativa. Se o usuário estiver ocioso por 10 minutos durante a sessão ativa, o uso líquido é de apenas 30 minutos.

- Na **Estratégia de gerenciamento de energia atual**, o uso líquido é de 60 minutos.
- Na **estratégia de desalocar máquinas no final da sessão**, o uso líquido, excluindo o tempo de desconexão, é de 40 minutos.
- Na **estratégia de desalocar máquinas para sessões inativas**, incluindo o tempo ocioso, o uso líquido é de 30 minutos.

Esses critérios servem como base para a análise. Essas estratégias ajudam a determinar o uso líquido das máquinas com mais precisão.

Consumo de máquinas e recomendações

A página **Modelagem de custos** fornece os seguintes detalhes sobre o consumo de máquinas e recomendações:

- **Gráfico de consumo de máquinas simultâneas**: Este gráfico exibe o uso de linha de base nos últimos 28 dias, com cada barra representando um dia da semana. A linha de base é calculada usando o percentil 75 (p75) de uso, uma métrica de agregação semelhante à média ou mediana. Por exemplo, para cada dia e hora, como terça-feira às 10h, a linha de base é determinada analisando o p75 dos dados das quatro terças-feiras anteriores às 10h. Esse processo é repetido para todas as horas e dias da semana. Passe o mouse sobre o gráfico para ver o número de máquinas consumidas na estratégia atual de gerenciamento de energia e na estratégia selecionada quando possíveis alterações no Autoscale forem aplicadas.
- **Oportunidade de economia**: Visualize as oportunidades de economia potenciais para Reservas do Azure e Planos de Economia para termos de um e três anos. A oportunidade de economia para as opções de **Compromisso** e **Pagamento conforme o uso** é exibida.
- **Recomendações**: Visualize as alterações recomendadas para Reservas do Azure e Planos de Economia. As recomendações incluem compromissos para cada plano para todas as combinações aplicáveis de séries, tipos e regiões de máquinas virtuais. Os dados estão disponíveis para termos de um e três anos.

Analisar por série de máquina virtual

Selecione a série de máquina virtual na lista suspensa para validar o número ideal de máquinas em relação ao custo por usuário. O custo por usuário por mês é uma estimativa do custo mensal projetado por usuário. Essa estimativa ajuda os clientes a entender o custo mensal projetado por usuário se eles reservarem um número específico de máquinas sob as Reservas do Azure ou se comprometerem com um valor específico em dólares por hora sob o **Plano de Economia**. Visualize o custo por usuário para Instâncias Reservadas do Azure e compromissos horários do Plano de Economia. O gráfico exibe pontos de dados para vários níveis de reserva (variando de

Sem Reserva a **Reserva Total**, incluindo **Reserva Ótima**) e níveis de compromisso de custo horário (variando de **Sem Compromisso** a **Compromisso Máximo**, incluindo **Compromisso Ótimo**).

A página **Modelagem de custos** fornece insights e recomendações valiosas para ajudar os clientes a otimizar suas cargas de trabalho do Azure e economizar custos. Ao analisar os padrões de uso e selecionar o plano apropriado, os clientes podem obter economias significativas.

Matriz de compatibilidade de recursos

O Citrix Monitor oferece suporte a três edições do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™). Elas são **Platinum**, **Citrix DaaS Advanced** e **Citrix DaaS Advanced Plus**. Recursos específicos do Citrix Monitor, versões de VDA, componentes dependentes e suas respectivas edições de licença estão listados na tabela a seguir.

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Suporte a seleção múltipla para grupos de entrega	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Tratamento aprimorado de alertas de balanceamento de carga vertical e horizontal	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Coleta aprimorada de métricas de rede para solução de problemas de sessão	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Observabilidade para VDA de múltiplas sessões	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Resumo de custos	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Monitoramento dos detalhes da duração do logon do VDA	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Descarte de alertas em massa	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Monitoramento aprimorado de métricas de rede no Citrix Monitor.	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Modelagem de custos para cargas de trabalho do Azure	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Opção para estender o monitoramento da otimização HDX além do	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Microsoft Teams				
Novas métricas no painel do Monitor, como "Total de usuários conectados" e "Versões do aplicativo Citrix Workspace encontradas em seu ambiente"	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Aprimoramentos na página de Economia de custos	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Métricas de integridade do Connector Appliance	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Melhoria no dimensionamento de carga de trabalho	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Melhoria na guia Desempenho da Sessão	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Economia de custos otimizando o	VDA 7 2212 executando	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
uso de armazenamento	Windows de 64 bits			
Melhorias nas ações do Monitor	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Opção para visualizar e solucionar problemas de sessões do Secure Private Access para implantações híbridas	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Integração com Webhook	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Relatório de aplicativos publicados menos usados e não utilizados	VDA 7 2212 executando Windows de 64 bits	Sim	Não	Não
Monitorar e solucionar problemas do Secure Private Access	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Guia Secure Private Access no Monitor	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Visibilidade para o serviço Secure Private Access	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Melhoria na guia Conexões	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Uso ativo da rede da máquina	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Métricas de integridade do Cloud Connector	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Exibindo detalhes da política em Eventos de Postura do Dispositivo	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Aprimoramento da página Tendências	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Exportar dados	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Configuração de webhook usando PowerShell SDK	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Gráficos de monitoramento de uso de aplicativos no Painel	VDA 7 2212 executando Windows de 64 bits	Sim	Não	Não
Integrações e exportações de dados	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Aprimoramento na triagem de problemas de carregamento de perfil de usuário	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Políticas de alerta avançadas	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Aprimoramentos no conteúdo do alerta	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Monitoramento de alerta de falha de sincronização de configuração do Cache de Host Local	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Alerta de ação de ligar falha e ação de desligar falha	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Política de infraestrutura (Pré-visualização)	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Monitoramento de infraestrutura (Pré-visualização)	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Opções para solucionar problemas quando os dados de ICA RTT ou Duração de Logon da Sessão não são preenchidos	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Melhoria na página de	VDA 7 2212 executando	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Economia de custos	Windows de 64 bits			
Diagnosticar sessões de usuário históricas (Pré-visualização)	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Alerta de tempo de atividade da máquina	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Dimensionamento de carga de trabalho	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Painel de atividades do Cache de Host Local	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Painel de Métricas de Desempenho Aprimoradas	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Visualização de Logon de Sessão Aprimorada	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Máquinas Não Registradas (em %)	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Otimização de Custos	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Inspecionar máquinas com ações de energia recentes	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Suporte para Microsoft Teams versão 2.1 ou anterior	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Suporte para HDX Plus para Windows 365 Cloud PCs e Azure Virtual Desktops	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Resumo das Métricas de Sondagem e dos Estágios de Falha da Sondagem	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Visualização de salto de rede de ponta a ponta	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Reproduzir sessões ao vivo e gravadas	VDA 7 2212 executando	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
	Windows de 64 bits			
Otimização do Microsoft Teams	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Progresso do envio de mensagem	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Suporte à autenticação do Citrix Probe Agent via Citrix Gateway com credenciais de domínio e autenticação multifator	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Topologia da Sessão	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Tendências para métricas de desempenho de sessão	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Monitorar várias instâncias do Citrix DaaS	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
(Pré-visualização)				
Visualizar o status do dispositivo de endpoint em Diagnósticos de Inicialização de Sessão usando Postura do Dispositivo	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Alerta de Máquinas com Falha	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Diagnóstico de Sessão de Pesquisa com nome de usuário	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Utilização de GPU em tempo real disponível para GPUs AMD	VDA 7 2212 executando Windows de 64 bits	Sim	Sim	Sim
Acessar Citrix Analytics for Performance - Detalhes da Sessão	Direito ao Citrix Analytics for Performance	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Reconexão Automática de Sessão	VDA 1906	Sim	Sim	Sim
Duração da Inicialização da Sessão	VDA 1903	Sim	Sim	Sim
Sondagem de Desktop	Citrix Probe Agent 1903	Sim	Não	Não
Duração do Citrix Profile Management no Carregamento de Perfil	VDA 1903	Sim	Sim	Sim
Detalhamento de Perfil	VDA 1811	Sim	Sim	Sim
Monitoramento de Alertas do Hypervisor	Nenhum	Sim	Não	Não
Sondagem de Aplicativos	Citrix Application Probe Agent 1811	Sim	Não	Não
Integridade da Licença RDS da Microsoft	VDA 7.16	Sim	Sim	Sim
Acesso ao console da máquina a	XenServer Hypervisor 7.3	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
partir do Monitor				
Exportação de Dados de Filtros	Nenhum	Sim	Sim	Sim
Detalhamento de Sessão Interativa	VDA 1808	Sim	Sim	Sim
Detalhes de GPO	VDA 1808	Sim	Sim	Sim
Dados Históricos da Máquina Disponíveis Usando a API OData	Nenhum	Sim	Sim	Sim
Políticas de Alerta Inteligente	Nenhum	Sim	Não	Não
Link do Assistente de Saúde	Nenhum	Sim	Sim	Sim
Detalhamento de Sessão Interativa	Nenhum	Sim	Sim	Sim
Análise de Aplicativos	VDA 7.15	Sim	Sim	Sim
API OData V.4	Nenhum	Sim	Sim	Sim

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Usuários VDA Linux Shadow	VDA 7.16	Sim	Sim	Sim
Acesso ao Console da Máquina	Nenhum	Sim	Sim	Sim
Monitoramento de Falhas de Aplicativo	VDA 7.15	Sim	Sim	Sim
Solução de Problemas Centrada em Aplicativos	VDA 7.13	Sim	Sim	Sim
Monitoramento de Disco	VDA 7.14	Sim	Sim	Sim
Monitoramento de GPU	VDA 7.14	Sim	Sim	Sim
Protocolo de Transporte no Painel de Detalhes da Sessão	VDA 7.13	Sim	Sim	Sim
Descrições de Falha de Conexão e Máquina Amigáveis ao Usuário	VDA 7.x	Sim	Sim	Sim
Retenção de Dados Históricos	VDA 7.x	Sim	Não	Não

CITRIX DAAS™

RECURSO	DEPENDÊNCIAS - VERSÃO MÍNIMA NECESSÁRIA	PLATINUM	CITRIX DAAS™ ADVANCED	CITRIX DAAS ADVANCED PLUS
Relatórios Personalizados	VDA 7.x	Sim	Não	Não
Relatórios de Utilização de Recursos	VDA 7.11	Sim	Sim	Sim
Alertas Estendidos para Condições de CPU, Memória e RTT ICA	VDA 7.11	Sim	Não	Não
Melhorias no Relatório de Exportação	VDA 7.x	Sim	Sim	Sim
Detalhes da Duração do Logon	VDA 7.x	Sim	Sim	Sim
Monitoramento e Alerta Proativos	VDA 7.x	Sim	Não	Não
Uso de Aplicativos Hospedados	VDA 7.x	Sim	Não	Não
Uso de SO de Sessão Única e Múltiplas Sessões	VDA 7.x	Sim	Não	Não
Suporte para Canal Virtual Framehawk	VDA 7.6	Sim	Sim	Sim

Pesquisa Agregada em várias instâncias DaaS

O Citrix DaaS permite que os clientes agreguem várias instâncias de seu serviço Citrix DaaS usando um modelo de hub e spoke. Com essa configuração, você pode usar o recurso de pesquisa universal para pesquisar usuários, máquinas, endpoints e transações em todos os locatários DaaS agregados.

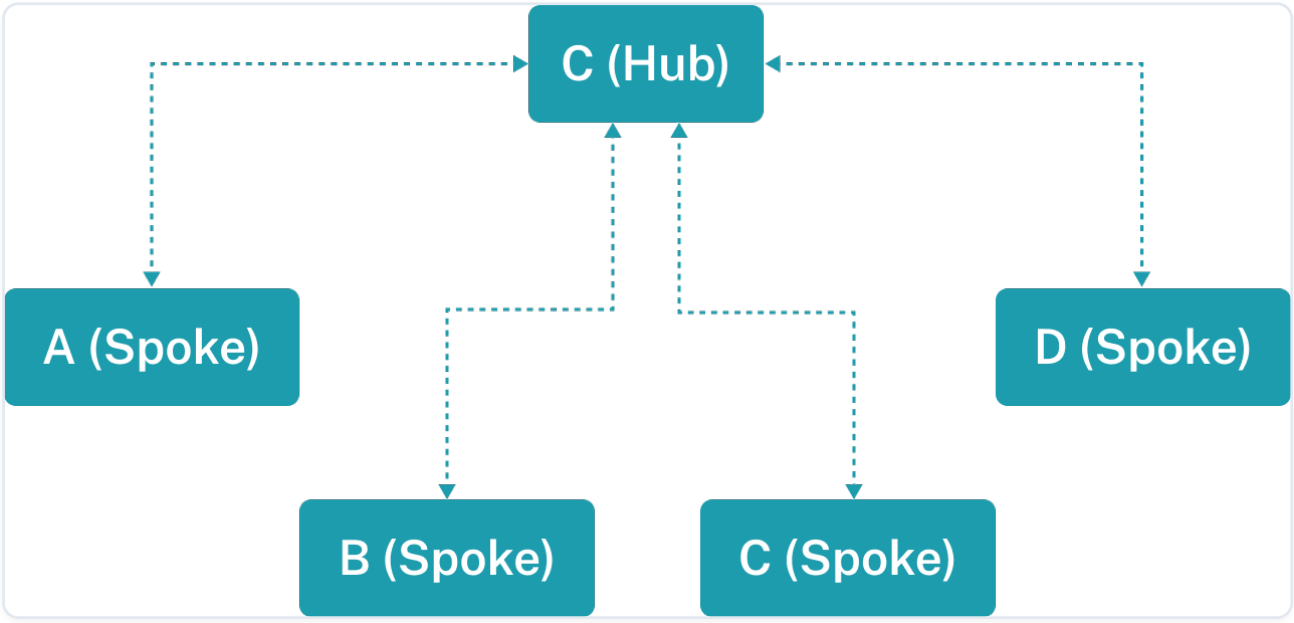
Pré-requisitos

Todos os locatários DaaS devem ser agregados usando uma topologia de hub e spoke. Para obter mais informações sobre a configuração necessária para agregar as instâncias de serviço spoke a um hub, consulte Agregar várias instâncias do Citrix DaaS.

> **Nota:**
>
> O Monitor oferece suporte à agregação de até quatro orgIDs DaaS (spokes) sob um único orgID (hub), permitindo que um total de 5 instâncias DaaS sejam monitoradas juntas.

Como funciona

Uma vez concluída a configuração de hub e spoke dos locatários DaaS, os administradores podem fazer login no console do Monitor de sua instância de hub configurada para pesquisar usuários, máquinas, endpoints e transações. A pesquisa agrega resultados do hub e de todos os seus spokes, apresentando resultados para solução de problemas adicionais.



Caso a enumeração bidirecional das instâncias de hub e spoke esteja configurada, os administradores podem fazer login no hub ou em qualquer um dos spokes para realizar a pesquisa.

Administração delegada

A administração delegada usa três conceitos: administradores, funções e escopos. As permissões são baseadas na função de um administrador e no escopo dessa função. Por exemplo, um administrador pode receber uma função de administrador de Help Desk onde o escopo envolve a responsabilidade por usuários finais em apenas um site.

As permissões administrativas determinam a interface de monitoramento apresentada aos administradores e as tarefas que eles podem realizar. As permissões determinam:

- As exibições que o administrador pode acessar, coletivamente referidas como uma exibição.
- Os desktops, máquinas e sessões que o administrador pode visualizar e interagir.
- Os comandos que o administrador pode executar, como sombrear a sessão de um usuário ou habilitar o modo de manutenção.

O Monitoramento agora oferece suporte a funções de administrador delegado que permitem atribuir funções personalizadas ou predefinidas a administradores. A função determina as permissões disponíveis e, portanto, como um administrador usa o monitoramento. Você também pode definir o escopo aplicável a essas funções. O escopo define os objetos para os quais a função é aplicável.

Para obter informações sobre como criar administradores delegados, consulte o artigo principal Administração delegada.

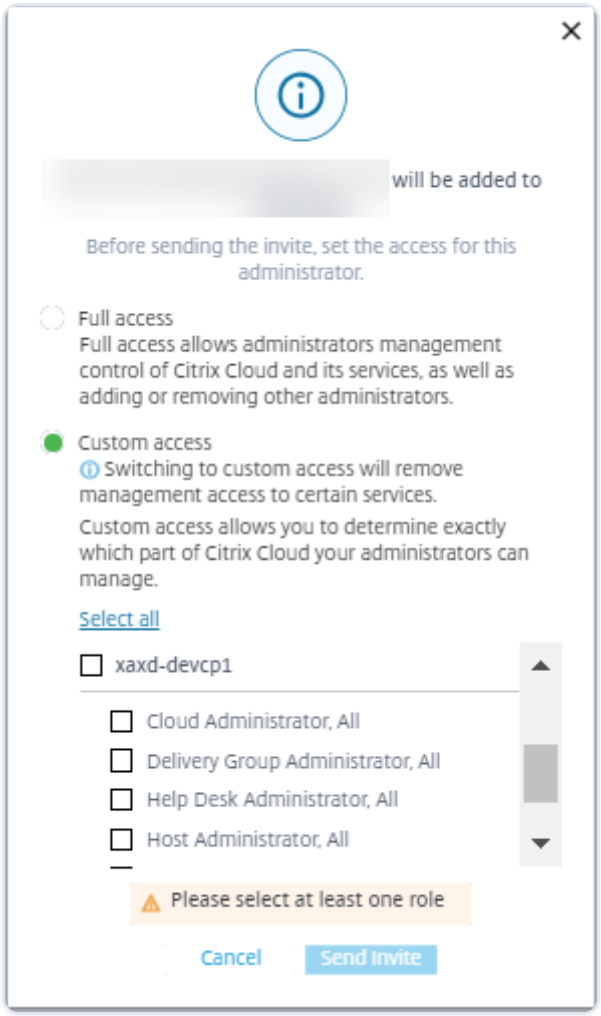
As funções e permissões predefinidas determinam como os administradores usam o **Monitor**:

FUNÇÃO DO ADMINISTRADOR	PERMISSÕES NO MONITOR
Administrador Completo	Acesso total a todas as exibições e pode executar todos os comandos, incluindo sombrear a sessão de um usuário, habilitar o modo de manutenção e exportar dados de tendências.
Administrador de grupo de entrega	Acesso total a todas as exibições e pode executar todos os comandos, incluindo sombrear a sessão de um usuário, habilitar o

FUNÇÃO DO ADMINISTRADOR	PERMISSÕES NO MONITOR
	modo de manutenção e exportar dados de tendências.
Administrador Somente Leitura	Pode acessar todas as exibições e ver todos os objetos em escopos especificados, além de informações globais. Pode baixar relatórios de canais HDX™ e exportar dados de Tendências usando a opção Exportar na exibição Tendências. Não pode executar outros comandos ou alterar nada nas exibições.
Administrador de Help Desk	Pode acessar apenas as exibições de Help Desk e Detalhes do Usuário e pode visualizar apenas objetos que o administrador está delegado a gerenciar. Pode acompanhar a sessão de um usuário e executar comandos para esse usuário. Pode executar operações de modo de manutenção. Pode usar opções de controle de energia para Máquinas OS de sessão única. Pode executar Tarefa de Script Incorporada. Pode executar Tarefa de Script Personalizada. Não pode acessar as exibições de Painel, Tendências, Alertas ou Filtros. Não pode usar opções de controle de energia para máquinas OS de várias sessões.
Administrador de catálogo de máquinas	Pode acessar apenas a página Detalhes da Máquina (pesquisa baseada em máquina).
Administrador de Host	Sem acesso. Este administrador não é compatível com o Monitor e não pode visualizar dados.
Administrador do Agente de Sondagem	Acesso somente leitura à página Aplicativos, não pode acessar nenhuma outra exibição. Destinado a executar o Agente de Sondagem Citrix em máquinas de endpoint.
Administrador Completo de Monitoramento	Tem acesso total a todas as exibições e comandos no console do **Monitor**.

FUNÇÃO DO ADMINISTRADOR	PERMISSÕES NO MONITOR
Administrador de Sessão	Pode visualizar Grupos de Entrega e gerenciar suas sessões e máquinas associadas na página **Filtros** do console do **Monitor**.

Para atribuir uma função (integrada ou personalizada) a um usuário, no menu Citrix Cloud™, vá para **Gerenciamento de Identidade e Acesso** > **Administradores**. Aqui, ao adicionar ou editar o acesso de um administrador, você pode selecionar **Acesso Personalizado** e uma das funções listadas.



Você pode definir funções e escopos personalizados em **Administrators > Administrators**.

As funções integradas e as funções personalizadas são listadas para seleção com escopo personalizado.

- [ ] [redacted]
  - [ ] Cloud Administrator, All
  - [ ] Delivery Group Administrator, All
  - [ ] Delivery Group Administrator, rds1DGAndCatalog
  - [ ] Delivery Group Administrator, vdaDGOnly
  - [ ] Full Monitor Administrator, All - Access to 'Monitor' tab only
  - [ ] Full Monitor Administrator, rds1DGAndCatalog - Access to 'Monitor' tab only
  - [ ] Full Monitor Administrator, vdaDGOnly - Access to 'Monitor' tab only
  - [ ] Help Desk Administrator, All - Access to 'Monitor' tab only
  - [ ] Help Desk Administrator, rds1DGAndCatalog - Access to 'Monitor' tab only
  - [ ] Help Desk Administrator, vdaDGOnly - Access to 'Monitor' tab only
  - [ ] Host Administrator, All
  - [ ] Host Administrator, rds1DGAndCatalog
  - [ ] Host Administrator, vdaDGOnly
  - [ ] Machine Catalog Administrator, All
  - [ ] Machine Catalog Administrator, rds1DGAndCatalog
  - [ ] Machine Catalog Administrator, vdaDGOnly
  - [ ] Probe Agent Administrator, All
  - [ ] Probe Agent Administrator, rds1DGAndCatalog
  - [ ] Probe Agent Administrator, vdaDGOnly
  - [ ] Read Only Administrator, All
  - [ ] Read Only Administrator, rds1DGAndCatalog
  - [ ] Read Only Administrator, vdaDGOnly
  - [x] TrendsFiltersAndUD, All
  - [ ] TrendsFiltersAndUD, rds1DGAndCatalog
  - [ ] TrendsFiltersAndUD, vdaDGOnly

Integrações e exportações de dados

O Citrix Monitor agora oferece uma nova interface de usuário para integrações e exportações de dados. Esse recurso ajuda a melhorar a conscientização sobre as várias interfaces e integrações de terceiros disponíveis no Citrix Monitor. A página **Integrações e exportações de dados** recém-introduzida lista o seguinte:

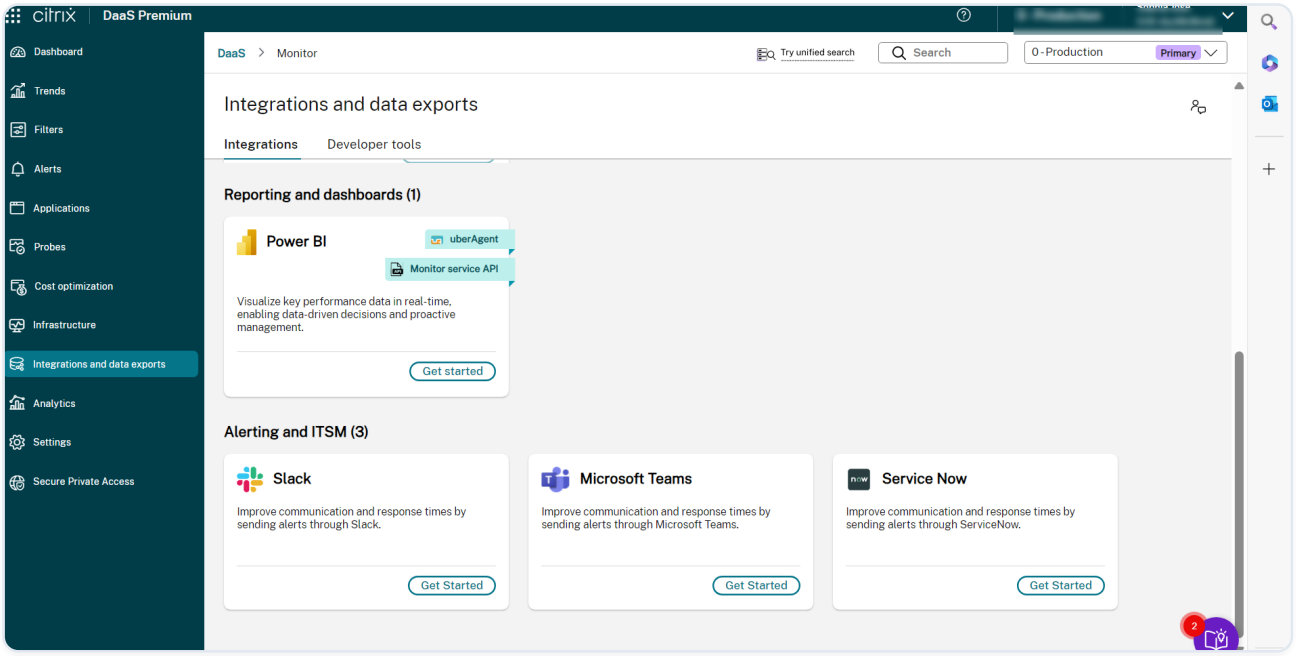
- Integrações disponíveis
- Ferramentas de desenvolvedor compatíveis

Esta página também descreve a configuração da API REST para exportação de dados. Além disso, fornece links de referência para os guias e documentos para começar com as integrações e ferramentas de desenvolvedor.

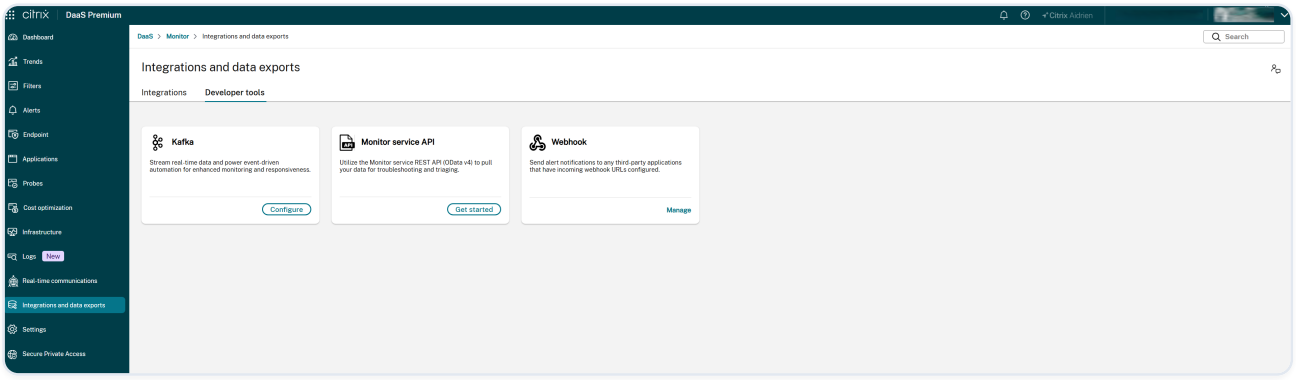
As seguintes opções de integração são fornecidas para coletar métricas de monitoramento do Citrix:

- API do serviço Citrix Monitor — Você pode usar a API do serviço Citrix Monitor para coletar dados de desempenho e eventos do Citrix Monitor e exportá-los para o Power BI.
- Alertas e ITSM — Você pode enviar notificações de alerta para os seguintes aplicativos de terceiros que têm URLs de webhook de entrada configuradas:
  - Slack
  - Microsoft Teams
  - ServiceNow

Clique em **Integrações e exportações de dados** no menu de navegação esquerdo. A página **Integrações e exportações de dados** é exibida.



Ferramentas de desenvolvedor:



Visualizar integrações disponíveis

A guia **Integrações** exibe as integrações disponíveis para o Citrix Monitor. As integrações disponíveis são categorizadas da seguinte forma:

- Relatórios e painéis
- Alertas e ITSM

Relatórios e painéis

O Power BI pode ser usado para visualizar métricas coletadas por meio da API do Citrix Monitor. Clique em **Começar**. A página de detalhes das ferramentas de desenvolvedor da **API REST** é exibida.

Clique em API do serviço Monitor para obter links de referência para recursos e blogs relacionados à sua integração com o PowerBI.

Esta página fornece links de referência para recursos e blogs.

Integrações com ferramentas de alerta e ITSM

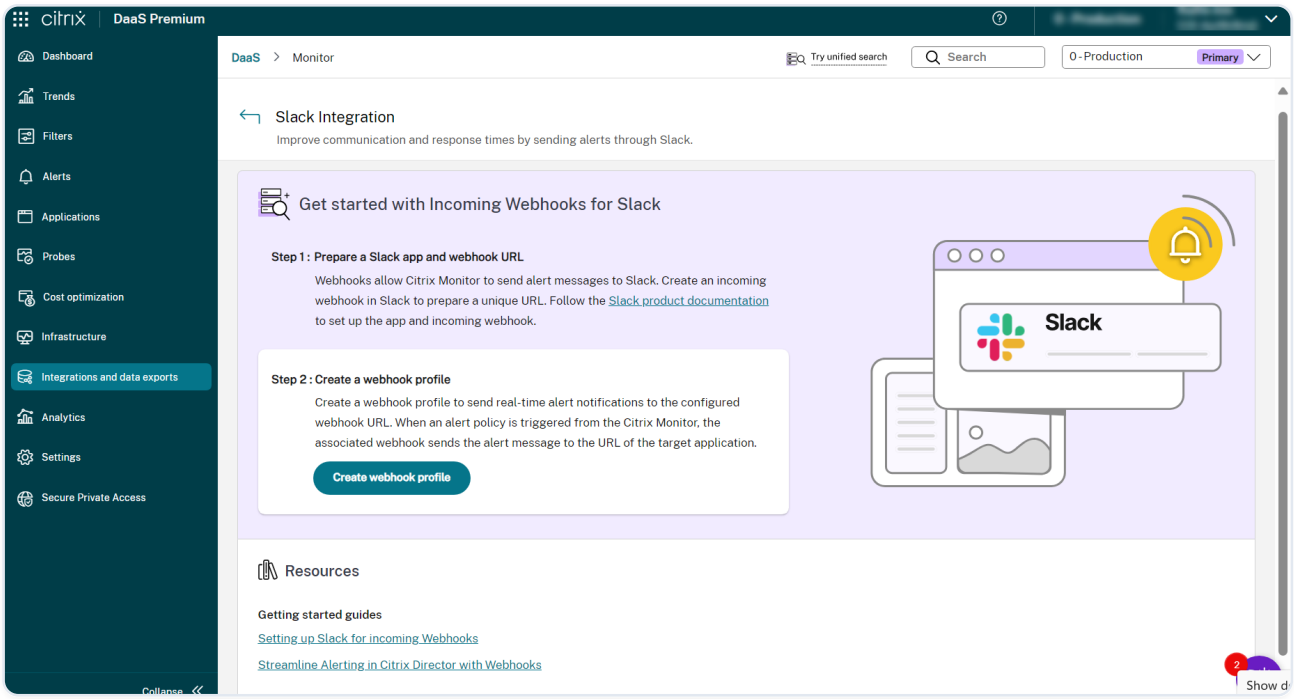
As ferramentas de alerta e ITSM incluem o seguinte:

- Slack
- Microsoft Teams
- ServiceNow

Para integrar as ferramentas de alerta e ITSM com o Webhook, clique no link **Começar** ao lado das ferramentas. Este link abre a página de integração para a ferramenta de alerta e ITSM específica, fornecendo detalhes sobre pré-requisitos e etapas específicas para enviar alertas. Você pode configurar as ferramentas e o URL do webhook. Por exemplo, para integrar o Slack, você precisa criar um canal e um URL de Webhook seguindo a documentação do Slack.

Feito isso, prossiga para a segunda etapa para criar um perfil de webhook.

Você também pode consultar os recursos de referência. Por exemplo, os pré-requisitos e as instruções para integração com o Slack são os seguintes:



Integração com Webhook

1. Clique na guia **Integrações** > seção **Alertas e ITSM** > **Começar** ao lado da ferramenta selecionada. A página **Integração** para essa ferramenta é aberta.
2. Você pode acessar os links de referência para recursos e blogs.
3. Siga a etapa 1.

4. Clique em **Criar perfil de webhook** como parte da etapa 2. A página `<name of the tool>` **Criar perfil de webhook** é exibida.
5. Insira o **Nome** do perfil de Webhook.
6. Insira a **Descrição** para o perfil de Webhook.
7. Selecione o **Método** desejado na seção **Configuração de webhook**.
8. Insira a URL da **API/Webhook** de acordo com o método selecionado na etapa anterior.
9. Visualize o formato da **Mensagem**.
10. Adicione a chave e o valor na seção **Cabeçalhos**.
11. Clique em **Testar** para validar o webhook criado.
12. Se o webhook for validado com sucesso, clique em **Criar Webhook**. O Webhook é criado.
13. Visualize os perfis de webhook criados em **Ferramentas de desenvolvedor** > **Webhook** > **Gerenciar**. A página **Detalhes da ferramenta de desenvolvedor de perfis de webhook** é aberta.

Você também pode criar perfis de webhook em **Ferramentas de desenvolvedor** > **Webhook** > **Criar perfis de webhook**.

Integrando os perfis de webhook com os alertas Citrix

Você pode visualizar os perfis de webhook criados na seção **Alertas** > **Políticas de alerta avançadas** > **Criar política** e usá-los como parte dos alertas Citrix.

Para integrar um perfil de webhook a uma nova política de alerta Citrix, faça o seguinte:

1. Clique em **Alertas** > **Políticas de alerta avançadas** > **Criar política**. A página **Criar política de alerta avançada** é exibida.
2. navegar até a seção **Canais de notificação** > **Usar Webhook**.
3. Selecione o perfil de webhook.
4. Salve a política de alerta.

Você pode integrar um perfil de webhook a uma política de alerta existente fazendo o seguinte:

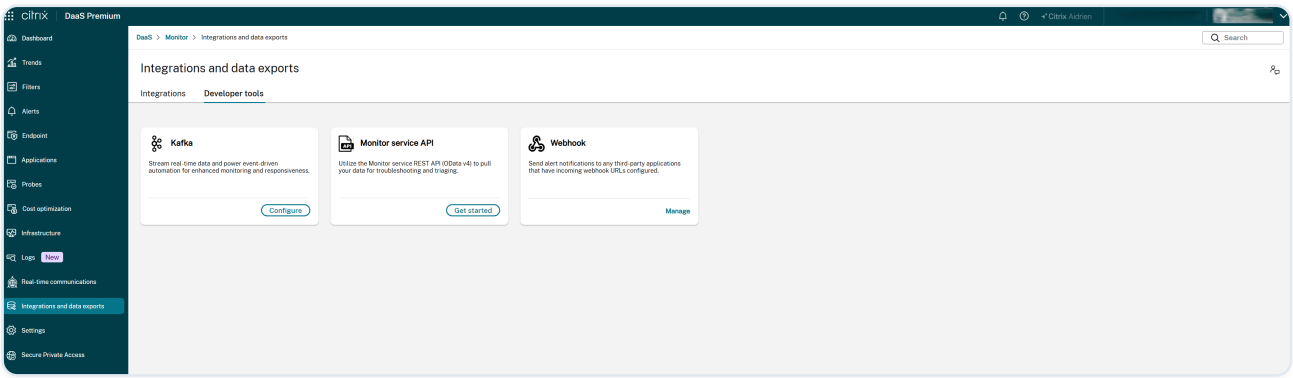
1. Clique em **Alertas** > **Políticas de alerta avançadas** > **Editar política**. A página **Editar política de alerta avançada** é exibida.
2. navegar até a seção **Canais de notificação** > **Usar Webhook**.
3. Selecione ou altere o perfil de webhook.

4. Atualize e salve a política de alerta.

Exibir ferramentas de desenvolvedor compatíveis

Clique na guia **Ferramentas do desenvolvedor** para visualizar as ferramentas do desenvolvedor disponíveis.

As ferramentas do desenvolvedor disponíveis são a API do serviço Monitor e o Webhook.



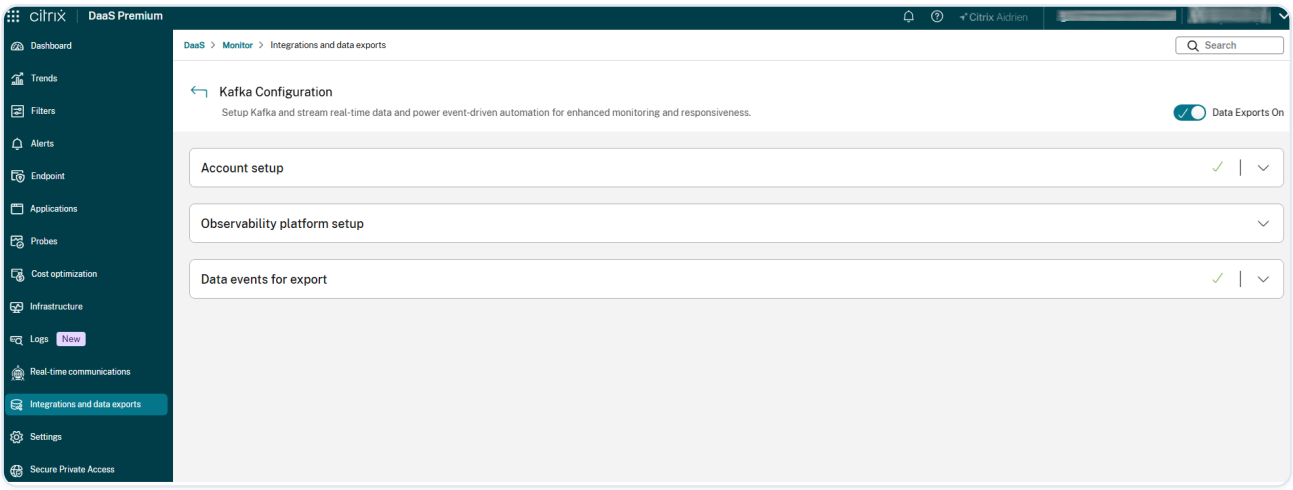
Exportações de Dados Kafka

As Exportações de Dados Kafka permitem que os administradores transmitam dados de eventos do Citrix Monitor para plataformas SIEM e de observabilidade externas, como Splunk, Elastic e Azure Sentinel. Os dados de eventos suportados incluem eventos do Secure Private Access (SPA) e do Device Posture Service (DPS).

Para acessar a configuração, use um dos seguintes caminhos:

- **Integrações e exportações de dados** > **Ferramentas do desenvolvedor** > **Kafka** na página **Integrações e exportações de dados**.
- **Secure Private Access** > **Kafka** no menu de navegação esquerdo.

A página **Configuração do Kafka** é exibida.



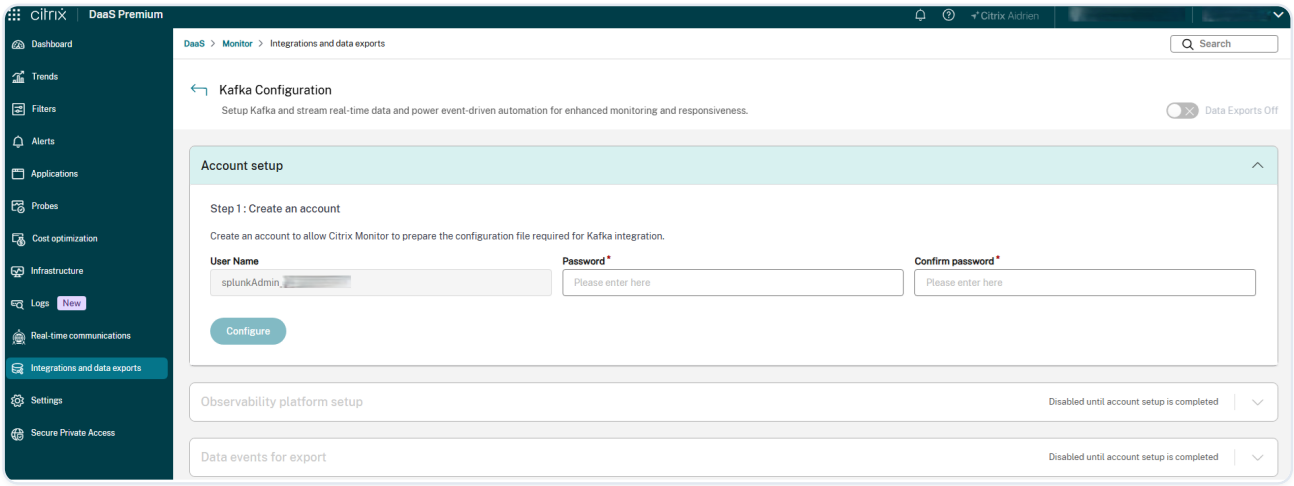
A página **Configuração do Kafka** contém três seções:

- **Configuração da conta** — Crie as credenciais da conta Kafka necessárias para a conectividade da ferramenta SIEM.
- **Configuração da plataforma de observabilidade** — Recupere os detalhes de conexão necessários para configurar sua plataforma de observabilidade escolhida.
- **Eventos de dados para exportação** — Selecione quais tipos de eventos são transmitidos para a plataforma de observabilidade.

Use o botão **Exportações de Dados** no canto superior direito para ativar ou desativar o fluxo de exportação a qualquer momento.

Configuração da conta

A seção **Configuração da conta** permite criar uma conta dedicada que o Citrix Monitor usa para gerar os arquivos de configuração necessários para a integração com o Kafka.



Para configurar a conta, faça o seguinte:

1. Expanda a seção **Configuração da conta**.
2. No campo **Senha**, insira uma senha para a conta. Insira a mesma senha em **Confirmar senha**.

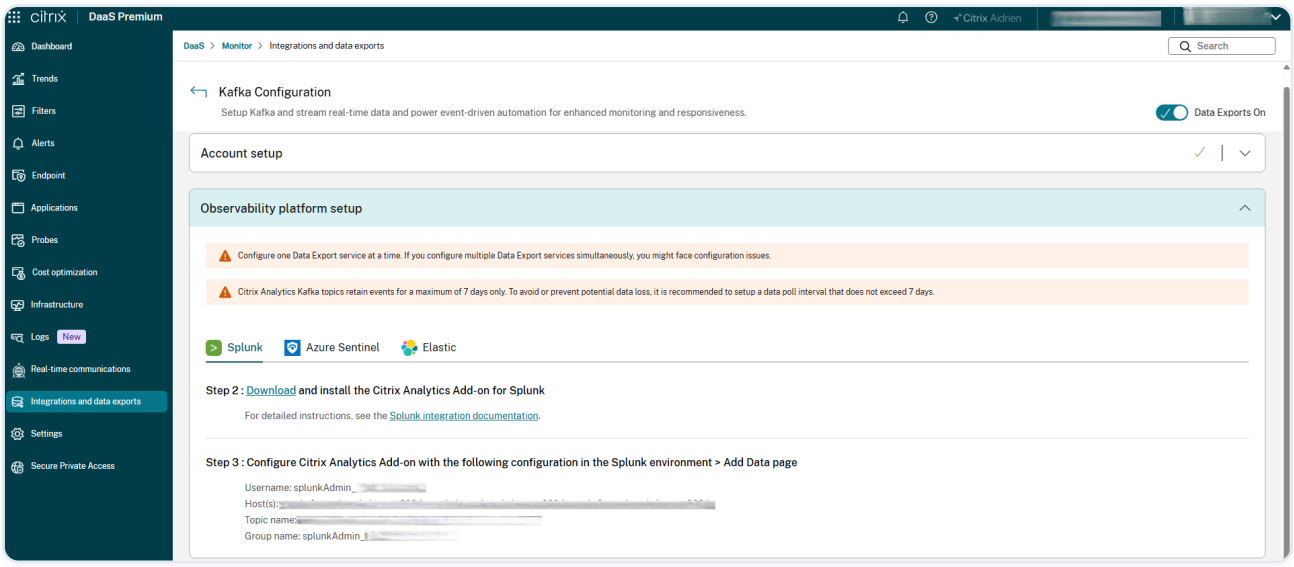
> **Nota:**
>
> O **Nome de usuário** é gerado automaticamente pelo Citrix Monitor e não pode ser editado.

3. Clique em **Configurar**. O Citrix Monitor cria a conta e prepara os arquivos de configuração.

Para atualizar a senha da conta a qualquer momento, clique em **Redefinir senha**, insira uma nova senha e clique em **Redefinir** novamente.

Configuração da plataforma de observabilidade

A seção **Configuração da plataforma de observabilidade** fornece os detalhes de conexão do Kafka necessários para configurar sua ferramenta SIEM ou de observabilidade.



As seguintes plataformas de observabilidade são compatíveis:

- **Splunk**
- **Azure Sentinel**
- **Elastic**

Para configurar sua plataforma de observabilidade, faça o seguinte:

1. Expanda a seção **Configuração da plataforma de observabilidade**.
2. Selecione a guia da sua plataforma de observabilidade (por exemplo, **Splunk**).
3. Siga as etapas na tela:

    - **Etapa 1:** Conclua a seção **Configuração da conta** para criar as credenciais da conta Kafka. Consulte Configuração da conta.
    - **Etapa 2:** Baixe e instale o Add-on do Citrix Analytics para sua plataforma. Para obter instruções detalhadas, consulte a documentação de integração vinculada na página.
    - **Etapa 3:** Use os detalhes de conexão exibidos na página para configurar o Add-on em seu ambiente de plataforma. Os detalhes incluem:

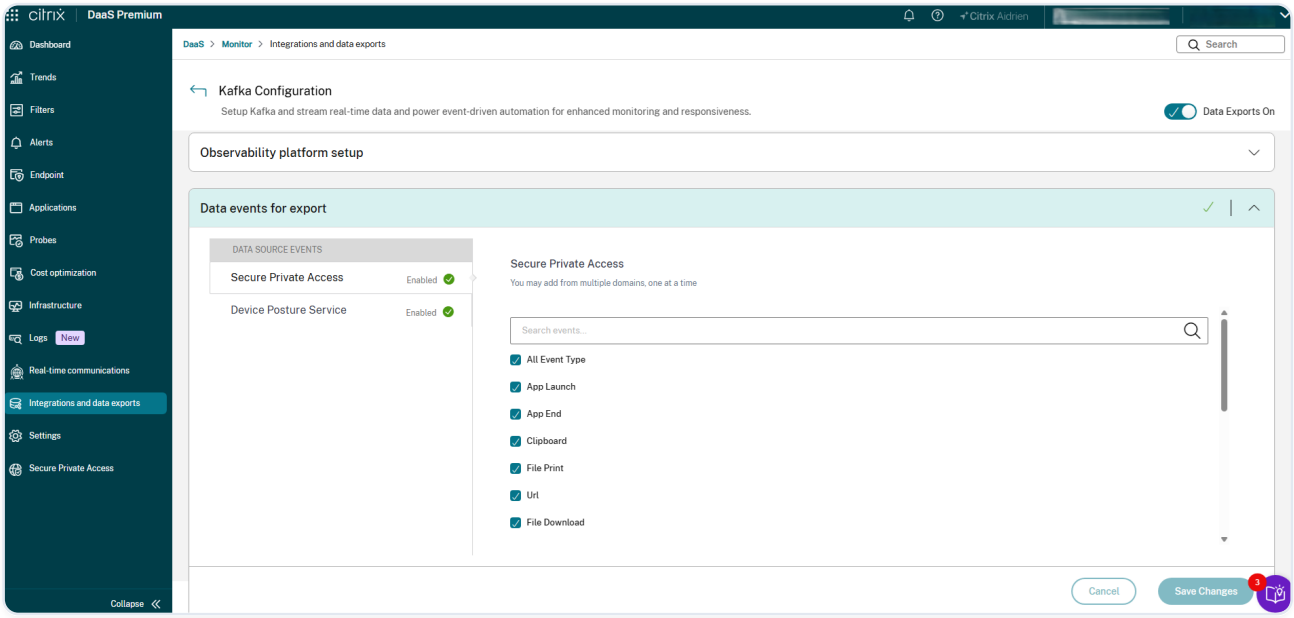
        - **Nome de usuário**

- **Host(s)**
- **Nome do tópico**
- **Nome do grupo**

Para **Azure Sentinel**, consulte integração do Microsoft Sentinel para obter instruções passo a passo.

Eventos de dados para exportação

A seção **Eventos de dados para exportação** permite escolher quais tipos de evento de cada fonte de dados são incluídos no fluxo de exportação.



As fontes de dados disponíveis são:

- **Secure Private Access** — Disponível para administradores com um direito de Secure Private Access. Os tipos de evento suportados incluem Início de Aplicativo, Fim de Aplicativo, Área de Transferência, Impressão de Arquivo, URL, Download de Arquivo e outros.
- **Device Posture Service** — Disponível para todos os administradores. Inclui eventos de Avaliação de Postura do Dispositivo.

Para configurar os tipos de evento para exportação, faça o seguinte:

1. Expanda a seção **Eventos de dados para exportação**.
2. No painel **Eventos da Fonte de Dados**, selecione uma fonte de dados (por exemplo, **Secure Private Access**).
3. No painel direito, selecione os tipos de evento a serem incluídos na exportação. Use o campo de pesquisa para filtrar eventos por nome. Selecione **Todos os Tipos de Evento** para incluir todos os eventos disponíveis para essa fonte.

4. Repita para cada fonte de dados conforme necessário.
5. Clique em **Salvar Alterações**.

API do serviço Monitor

Clique em **Começar**. A página de detalhes da ferramenta de desenvolvedor **API do Serviço Monitor** é aberta. Você pode acessar os links de referência para recursos e blogs.

Webhook

Você pode visualizar e criar perfis de webhook em **Ferramentas de desenvolvedor** > **Webhook** > **Criar perfis de webhook**.

Integração com o Microsoft Sentinel

As Exportações de Dados Kafka no Citrix® Monitor podem transmitir eventos de **Secure Private Access (SPA)** e **Device Posture Service (DPS)** para o Microsoft Sentinel através do Logstash. O **Citrix SPA Sentinel App** no hub de Conteúdo do Microsoft Sentinel fornece o conector de dados e as informações de conexão que o Logstash precisa para encaminhar os eventos.

Para integrar com o Microsoft Sentinel, instale a solução Citrix SPA Sentinel App do hub de Conteúdo e configure o Logstash, conforme descrito nas seções a seguir.

Pré-requisitos

- Um espaço de trabalho do Microsoft Sentinel e permissão para instalar uma solução do hub de Conteúdo.
- Um host Logstash executando uma versão do Logstash compatível com o plug-in de saída do Microsoft Sentinel. Para as versões compatíveis, consulte Pré-requisitos do plug-in Logstash.
- Certifique-se de que os endpoints do broker de Exportações de Dados Kafka para sua região estejam na lista de permissões em sua rede:

ENDPOINT	REGIÃO DOS ESTADOS UNIDOS	REGIÃO DA UNIÃO EUROPEIA	REGIÃO DA ÁSIA-PACÍFICO SUL
Brokers Kafka	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`

ENDPOINT	REGIÃO DOS ESTADOS UNIDOS	REGIÃO DA UNIÃO EUROPEIA	REGIÃO DA ÁSIA-PACÍFICO SUL
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`		

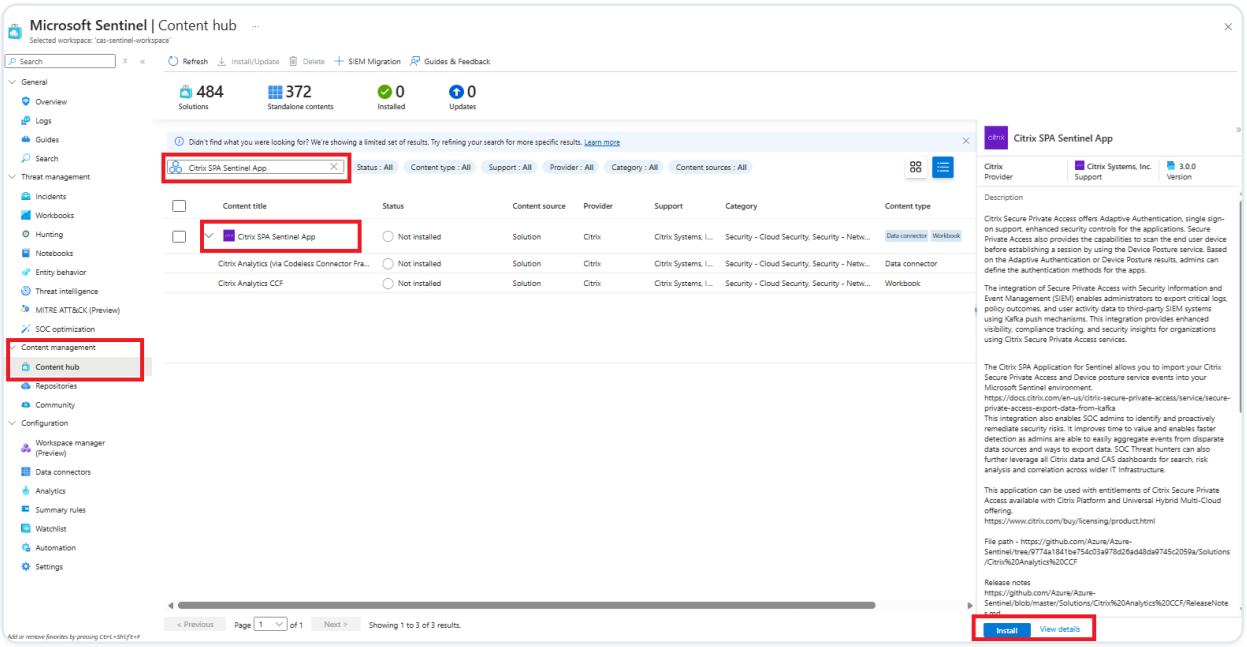
Para validar a conectividade de rede com um broker Kafka, execute os seguintes comandos em seu ambiente e confirme que eles são bem-sucedidos. Substitua o endpoint por um broker para sua região.

```
telnet casnb-0.citrix.com 9094

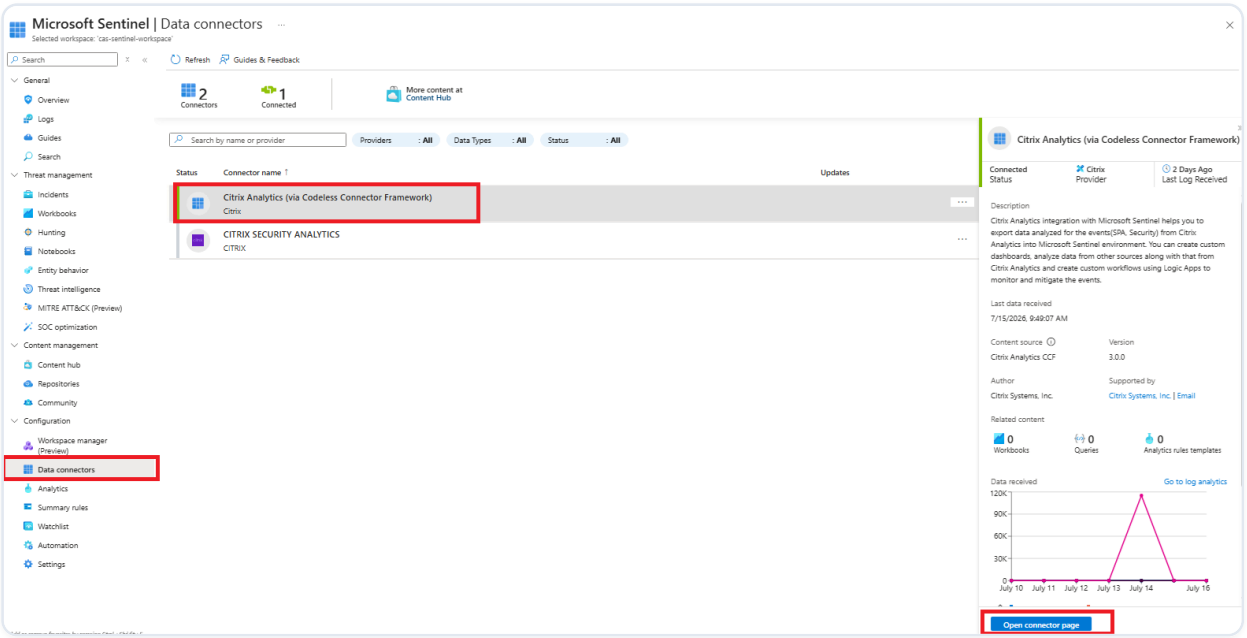
openssl s_client -tls1_3 -connect casnb-0.citrix.com:9094 -showcerts
< /dev/null
```

Instalar o aplicativo Citrix SPA Sentinel

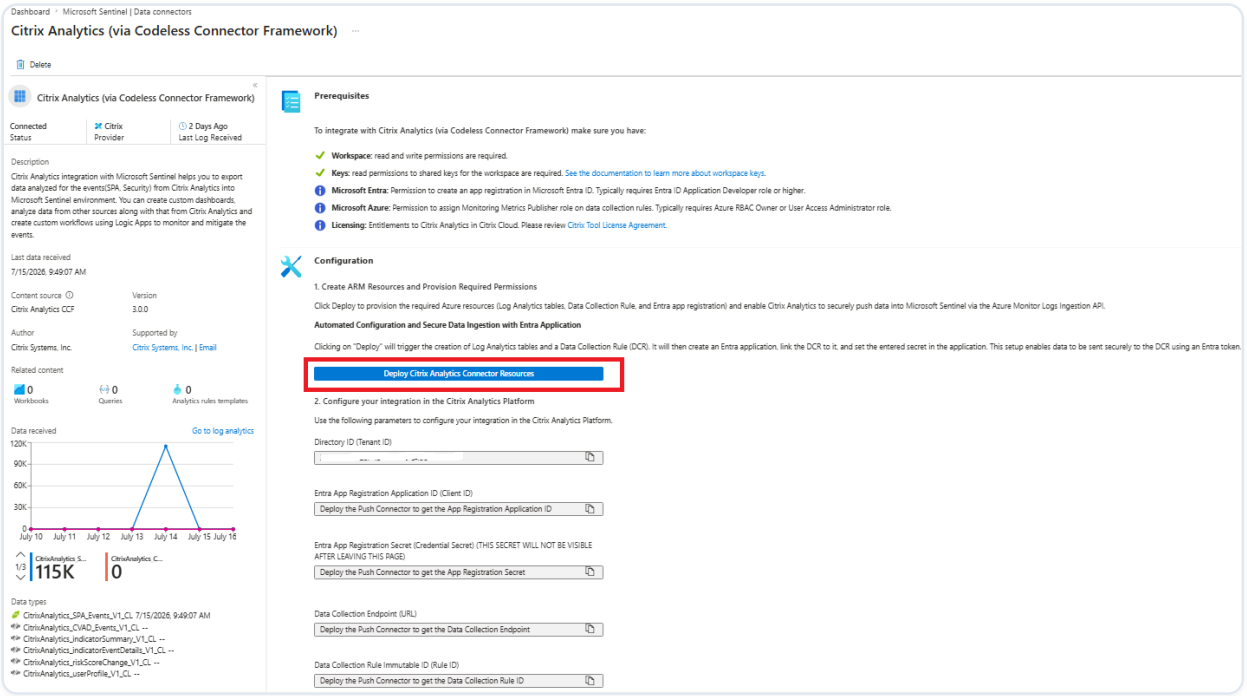
1. No portal do Azure, abra o **Microsoft Sentinel** e selecione seu espaço de trabalho.
2. Em **Gerenciamento de conteúdo**, clique em **Hub de conteúdo**.
3. Procure por **Citrix SPA Sentinel App** e clique em **Instalar**.



4. Vá para **Configuração** > **Conectores de dados** e abra o conector de dados fornecido com a solução. Clique em **Abrir página do conector**.



5. Implante os recursos do conector, incluindo a regra de coleta de dados (DCR) e o aplicativo Microsoft Entra usado para autenticação. Quando a implantação terminar, mantenha as **informações de conexão** mostradas na página do conector de dados abertas — você as colará na configuração do Logstash na próxima etapa.



> **Nota:**
>
> Por motivos de segurança, o **Segredo de Registro do Aplicativo Entra** é mostrado apenas uma vez. Ele não será mais visível depois que você sair ou atualizar a página do conector de dados. Enquanto os recursos estão sendo implantados, copie e salve o segredo assim que ele aparecer. Se o **Segredo de Registro do Aplicativo Entra** desaparecer antes de você copiá-lo, clique em **Revogar acesso** para excluir o aplicativo Entra e remover o conector de dados e, em seguida, implante os recursos do conector novamente para gerar um novo segredo.

Configurar o Logstash

1. No Citrix Monitor, abra **Integrações e exportações de dados** > **Ferramentas de desenvolvedor** > **Kafka** para exibir a página **Configuração do Kafka**, então crie a conta e baixe os arquivos de configuração:

   a. Preencha a seção **Configuração da conta** para criar as credenciais da conta Kafka. Para as etapas detalhadas, consulte Configuração da conta.

   b. Expanda a seção **Configuração da plataforma de observabilidade** e selecione a guia **Azure Sentinel**.

   c. Baixe o arquivo de configuração do Logstash e o truststore JKS gerados para sua conta.

2. No host do Logstash, instale o Logstash e o plug-in de saída do Microsoft Sentinel.

3. Na máquina host onde você instalou o Logstash, coloque os arquivos baixados no diretório especificado:

TIPO DE MÁQUINA HOST	NOME DO ARQUIVO	CAMINHO DO DIRETÓRIO
Linux	DIRECTOR_AzureSentinel_LogStash_Config.conf	Para pacotes Debian e RPM: `/etc/logstash/conf.d/`
		Para arquivos .zip e .tar.gz: `{extract.path}/config`
	kafka.client.truststore.jks	Para pacotes Debian e RPM: `/etc/logstash/ssl/`
		Para arquivos .zip e .tar.gz: `{extract.path}/ssl`
Windows	DIRECTOR_AzureSentinel_LogStash_Config.conf	`C:\logstash-x.xx.x\config`
	kafka.client.truststore.jks	

4. Abra o arquivo de configuração do Logstash e faça o seguinte:

   a. Na seção de entrada do arquivo, insira o seguinte:

   - **Senha**: A senha da conta que você criou durante a Configuração da conta no Citrix Monitor (**Integrações e exportações de dados** > **Ferramentas de desenvolvedor** > **Kafka**).
   - **Local do truststore SSL**: O local do seu certificado de cliente SSL. Este é o local do arquivo kafka.client.truststore.jks na sua máquina host.

```
input {
  kafka {
    bootstrap_servers => "casnb-0.citrix.com:9094,casnb-1.citrix.com:9094,casnb-2.citrix.com:9094,casnb-3.citrix.com:9094"
    topics => ["cas.siem.aec719c5-035e-40bb-87f9-310dd1f1de29"]
    group_id => "splunkAdmin_ab2wib4x8s6a-group"
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='splunkAdmin_ab2wib4x8s6a' password='<your password>';"
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
}
```

   b. Na seção **output (Microsoft Sentinel)**, cole as informações de conexão da etapa 5 de Install the Citrix SPA Sentinel App — o endpoint de coleta de dados (DCE), o ID imutável

da regra de coleta de dados (DCR) e as credenciais do aplicativo Entra (ID do locatário, ID do cliente e o segredo de registro do aplicativo Entra).

```
output {
  if [event_type] in ["datasourceSPAEventDetails", "datasourceDPSEventDetails"] {
    microsoft-sentinel-log-analytics-logstash-output-plugin {
        client_app_Id => "<application id>"
        client_app_secret => "<application secret>"
        tenant_id => "<tenant id>"
        data_collection_endpoint => "<data collection endpoint>"
        dcr_immutable_id => "<data collection rule id>"
        dcr_stream_name => "Custom-CitrixAnalytics_SPA_Events_V1"
    }
  }
}
```

5. Reinicie o Logstash para aplicar a configuração.

Selecione os tipos de evento SPA e DPS

Escolha os tipos de evento que o Kafka Data Exports transmite para o Sentinel em **Eventos de dados para exportação** na página Kafka Data Exports:

- **Secure Private Access** — Inicialização de aplicativo, Encerramento de aplicativo, Área de transferência, Impressão de arquivo, URL, Download de arquivo e tipos de evento relacionados.
- **Device Posture Service** — Eventos de avaliação de postura do dispositivo.

Para obter informações sobre a exportação upstream do Kafka, consulte Export data from Kafka for Secure Private Access.

Verificar a ingestão de dados

Depois que o Logstash começar a encaminhar, os eventos aparecerão em seu espaço de trabalho do Microsoft Sentinel em alguns minutos. Verifique o indicador **Dados recebidos** na página do conector de dados para confirmar que a ingestão foi iniciada.

Para confirmar que os eventos estão chegando à tabela, abra **Microsoft Sentinel** > **Logs** e execute a seguinte consulta:

```
CitrixAnalytics_SPA_Events_V1_CL

| where TimeGenerated > ago(24h)

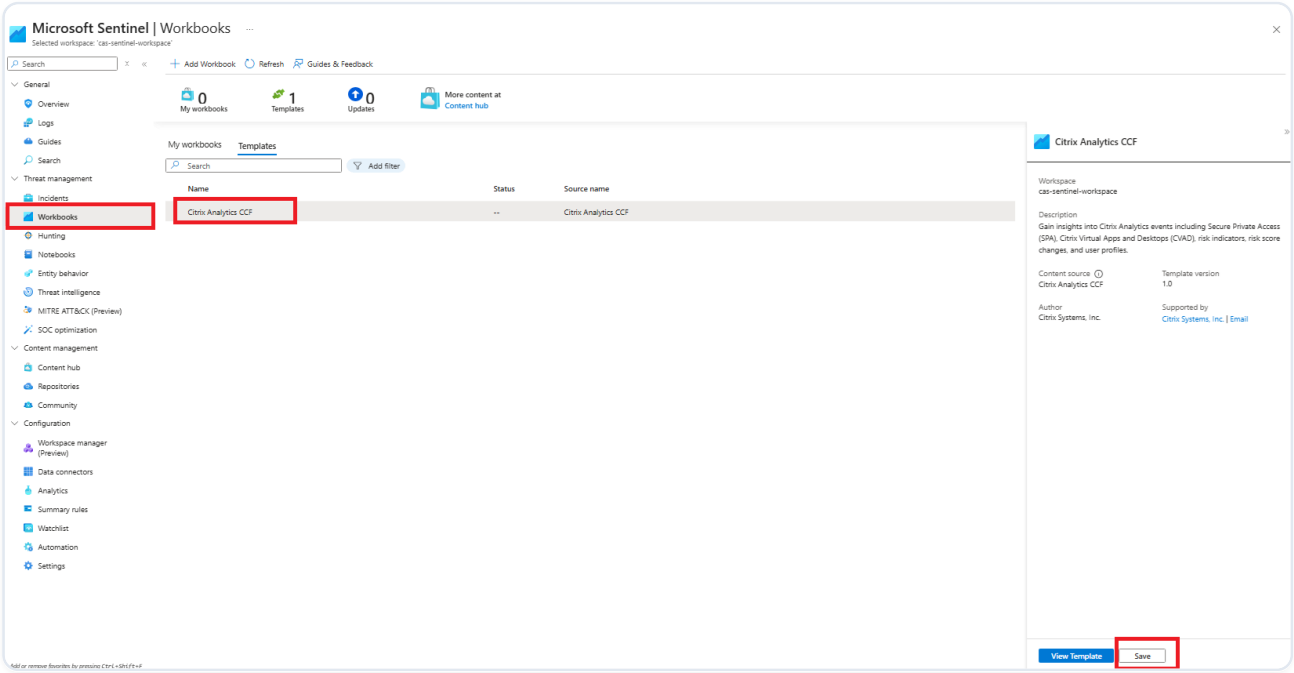
| summarize count() by event_type, event_category
```

```
| order by count_ desc
```

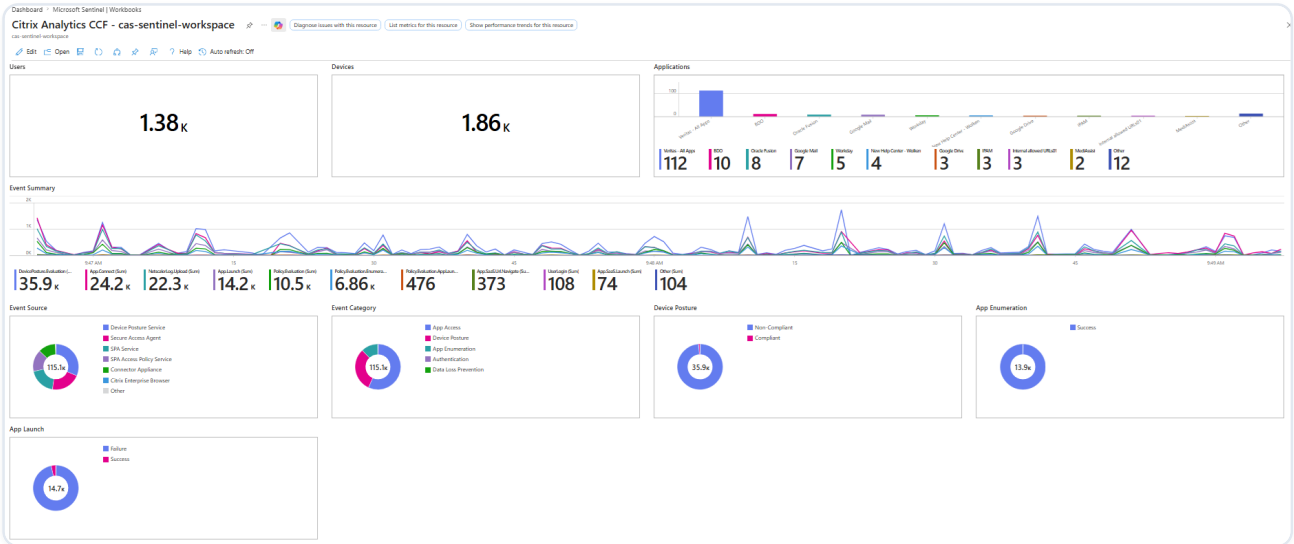
A consulta retorna a contagem de eventos das últimas 24 horas, agrupados por tipo e categoria de evento. Se retornar resultados, os dados estão sendo ingeridos com sucesso.

Exibir pasta de trabalho

O aplicativo Citrix SPA Sentinel vem com um modelo de pasta de trabalho. Para usá-lo, abra **Microsoft Sentinel** > **Gerenciamento de ameaças** > **Pastas de trabalho** > **Modelos**, selecione a pasta de trabalho **Citrix Analytics CCF** e clique em **Salvar**. Em seguida, selecione **Exibir pasta de trabalho salva** para abri-la.



O livro de trabalho fornece uma guia **Secure Private Access** que visualiza a atividade de SPA e DPS.



O modelo do livro de trabalho é um ponto de partida. Como todos os eventos são armazenados na tabela `CitrixAnalytics_SPA_Events_V1_CL`, você também pode criar suas próprias visualizações adaptadas às suas necessidades — escreva consultas Kusto personalizadas e crie livros de trabalho ou painéis que destaquem as métricas e os insights mais relevantes para sua organização.

Acesso Privado Seguro

O Citrix Monitor permite que o administrador de help desk ou o administrador completo monitore e solucione problemas de todas as sessões de Acesso Privado Seguro.

Para começar a monitorar as sessões de Acesso Privado Seguro em seu site, consulte o seguinte:

- Guia Acesso Privado Seguro(/pt-br/citrix-daas/monitor/secure-private-access/secure-private-access-tab.html)
- Monitorar e solucionar problemas de Acesso Privado Seguro(/pt-br/citrix-daas/monitor/secure-private-access/spa-integration-with-monitor.html)
- Alertas de Acesso Privado Seguro(/pt-br/citrix-daas/monitor/site-analytics/alerts-notifications.html#alerts-for-spa-connection-latency)

Guia Secure Private Access no Monitor

A guia **Secure Private Access** no Monitor oferece um local dedicado para todos os novos recursos relacionados ao Secure Private Access. Esta guia fornece detalhes sobre as funções suportadas para o Secure Private Access, dando aos administradores um local central para acessar e gerenciar esses recursos.

Principais benefícios

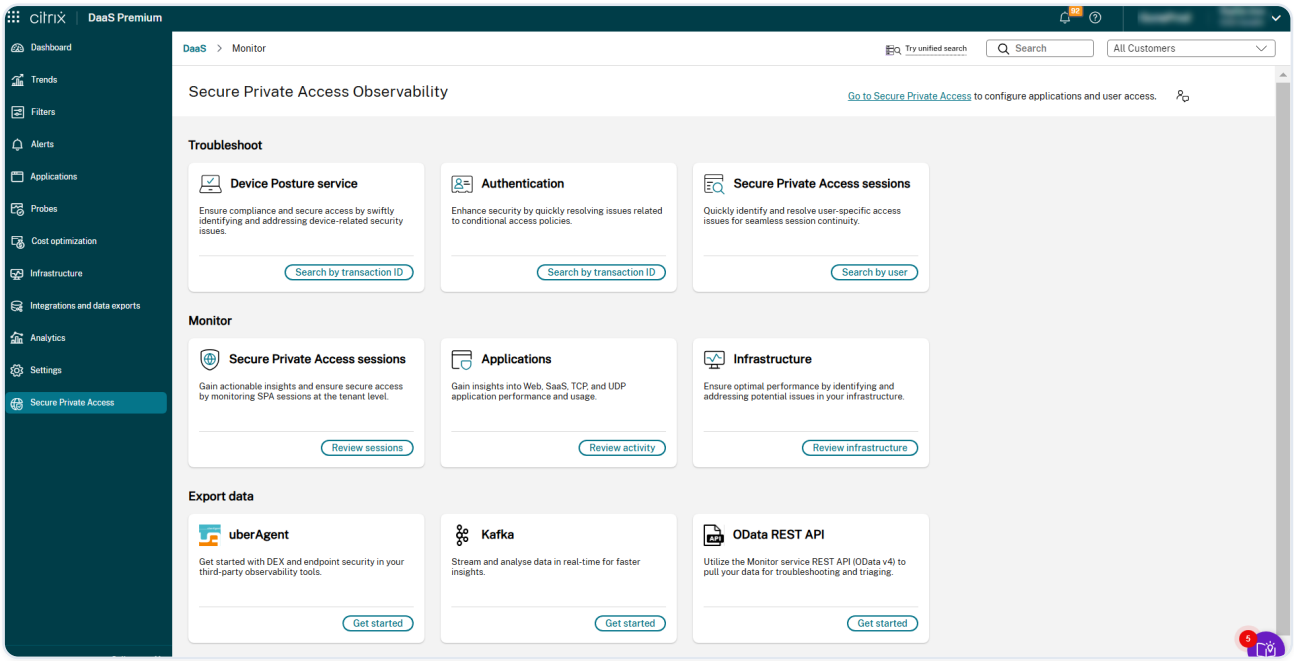
- Informações centralizadas: Os administradores podem ver facilmente todos os recursos de solução de problemas suportados para o Secure Private Access em um só lugar.
- Observabilidade aprimorada: A nova barra de navegação esquerda na interface do usuário do Monitor lista todos os serviços do Secure Private Access, incluindo sessões, aplicativos e postura do dispositivo do Secure Private Access, proporcionando melhor observabilidade.
- Navegação aprimorada: A guia Secure Private Access inclui hiperlinks para diferentes páginas, facilitando para os administradores navegar para vários recursos e funções.

Requisitos

- A guia **Secure Private Access** é visível para todos os administradores de clientes.

- Os cartões específicos do Secure Private Access (sessões e aplicativos do Secure Private Access) são clicáveis apenas quando o cliente tem direito ao Secure Private Access e o administrador tem permissões de administrador completo ou administrador somente leitura do Secure Private Access.

Para visualizar a página **Secure Private Access**, clique na guia **Secure Private Access** na interface do usuário do Monitor.



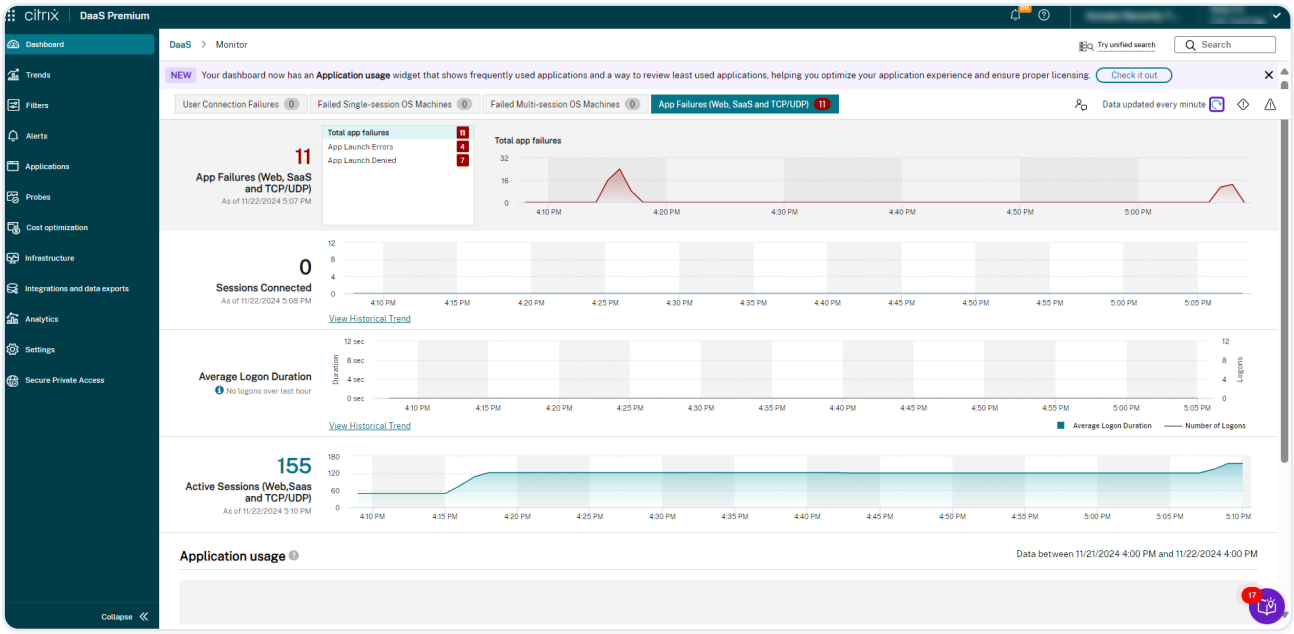
Visibilidade para o Serviço Secure Private Access

Para fornecer monitoramento e visibilidade detalhados para aplicativos e usuários do Secure Private Access, o Monitor foi aprimorado para incluir a visibilidade da sessão do Secure Private Access. A guia **Filtros** e o **Painel** fornecem informações detalhadas da sessão do Secure Private Access.

Principais recursos

- **Filtrar Sessões do Secure Private Access**: Agora você pode filtrar as sessões do Secure Private Access na guia **Filtros** > **Sessões (Web, SaaS e TCP/UDP)**.
- **Filtrar Aplicativos Secure Private Access**: Você também pode filtrar aplicativos Secure Private Access na guia **Filtros** > **Aplicativos (Web, SaaS e TCP/UDP)**.
- **Falhas de Aplicativos e Sessões Ativas**: Monitore falhas de aplicativos para aplicativos web/SaaS e TCP/UDP, e visualize sessões ativas para aplicativos web/SaaS no Painel.

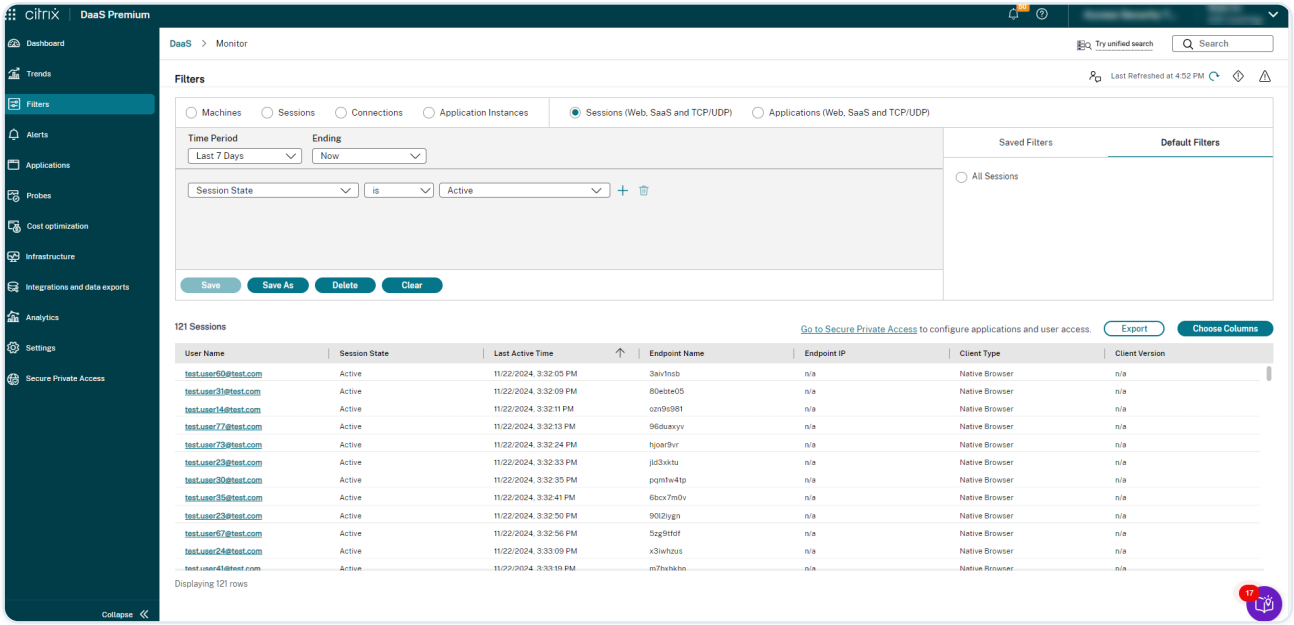
Painel:



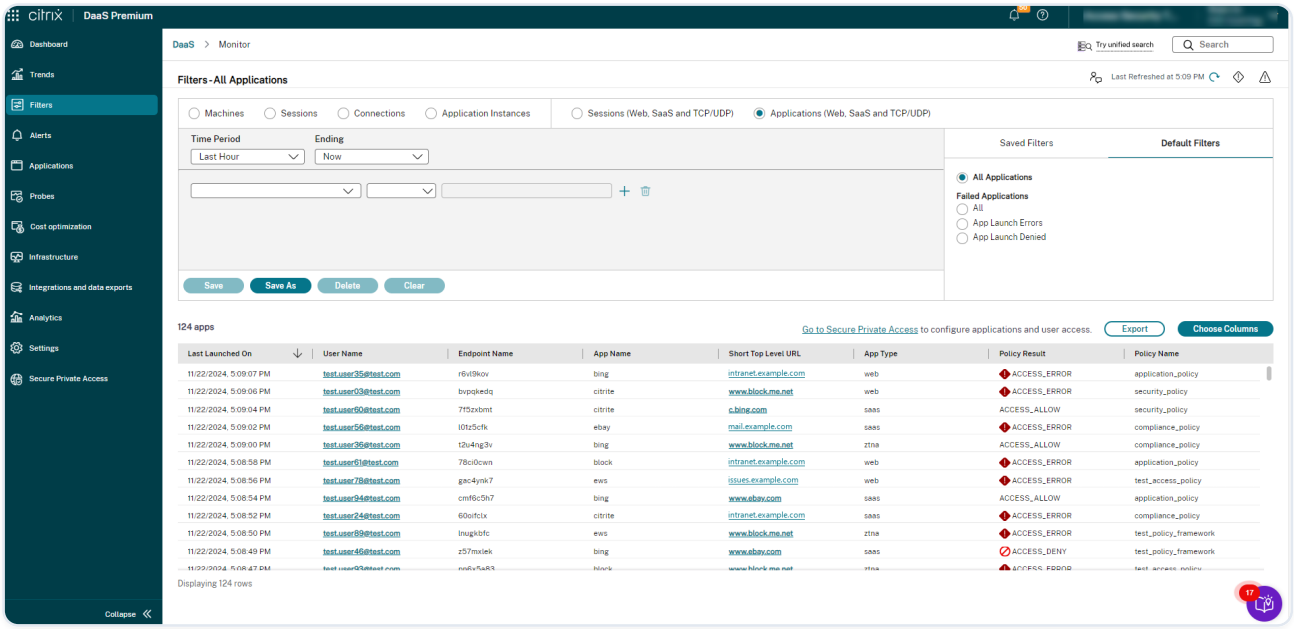
Nota:

- O número exibido no painel ao lado de Falhas de Aplicativos (Web, SaaS e TCP/UDP) representa o número de falhas de aplicativos na última hora.
- O número exibido no painel ao lado de Sessões Ativas (Web, SaaS e TCP/UDP) representa o número atual de sessões ativas do Secure Private Access na última hora.

Filtrar todas as Sessões do Secure Private Access:



Filtrar todos os Aplicativos do Secure Private Access:



Monitorar e solucionar problemas do Secure Private Access

O Secure Private Access é integrado ao Monitor, o console de monitoramento e solução de problemas do Citrix DaaS. Administradores e pessoal de suporte técnico podem monitorar e solucionar problemas de sessões e eventos de aplicativos Web/SaaS e TCP/UDP a partir do DaaS Monitor, além do painel do Secure Private Access.

Direitos de serviço

Para usar o recurso DaaS Monitor com o Secure Private Access, você deve ter direitos de Secure Private Access e de DaaS.

Clientes suportados

- Aplicativo Citrix Workspace™ - 2409 e posterior
- Citrix Secure Access para Windows - 24.8.1.19 e posterior
- Citrix Secure Access para macOS - 24.10.1 e posterior

Como acessar o Monitor

Você pode acessar o Monitor a partir do painel do Secure Private Access (**Ir para o Monitor**) ou do bloco de serviço do Citrix DaaS™.

Definições de sessão

Uma sessão do Secure Private Access oferece um resumo abrangente do ciclo de vida da sessão de um usuário final, atividade do aplicativo e experiência do usuário em um dispositivo específico.

Uma sessão serve como um registro unificado para solução de problemas e análise, fornecendo visibilidade sobre os seguintes aspectos:

- Insights detalhados sobre como os aplicativos são acessados, incluindo saltos de inicialização, topologia de rede, conexões e detalhes de roteamento. Esses detalhes são cruciais para resolver problemas relacionados a políticas de acesso.
- Rastreia toda a atividade da sessão de:
    - Navegadores acessando aplicativos web ou SaaS.
    - O cliente Citrix Secure Access para aplicativos privados usando protocolos TCP/UDP.

Algumas das principais características de uma sessão do Secure Private Access são:

- Cada sessão recebe um ID exclusivo para rastreamento e análise.
- Uma única sessão pode incluir vários lançamentos de aplicativos e fornece uma visão abrangente da atividade do usuário dentro dessa sessão específica.
- Para cada aplicativo, a sessão rastreia:
    - Os controles de segurança que se aplicam ao aplicativo.
    - O nome de exibição e o ID da política que acionaram os controles de segurança.
    - A condição que resultou na aplicação da política.
- A sessão rastreia todos os domínios internos que um usuário visitou no Citrix Enterprise Browser™ fornecendo insights sobre a navegação do usuário dentro do ambiente seguro.

Sessões de aplicativos Web/SaaS

O início e o fim da sessão para aplicativos Web/SaaS são definidos da seguinte forma:

- Início: O Citrix Enterprise Browser ou o Chrome Enterprise Premium é aberto no aplicativo Citrix Workspace e os aplicativos são acessados.
- Fim: Uma sessão termina nos seguintes cenários.
    - Você fecha o Citrix Enterprise Browser.
    - Após 30 minutos de inatividade e nenhuma atividade de sessão ser relatada.

      O cliente Citrix Enterprise Browser/Chrome Enterprise Premium envia uma atividade de sessão a cada 15 minutos para o Monitor. Se esta atividade de sessão não for recebida por 30 minutos, o que pode ocorrer devido aos seguintes motivos:
        - Falha de rede.

- Problemas de conectividade com a Internet.
- Fechamento da sessão após o intervalo de 360 minutos sem atividade de sessão.

> **Nota:**
>
> Para aplicativos iniciados por meio de navegadores nativos (sem agente), a sessão termina após 120 minutos de inatividade.

Sessões de aplicativos TCP/UDP

O início e o fim da sessão para aplicativos TCP/UDP são definidos da seguinte forma:

- Início: Você faz login no cliente Citrix Secure Access™ e acessa os aplicativos.
- Fim: Uma sessão termina nos seguintes cenários.
  - Você faz logout do cliente Citrix Secure Access.
  - Após 30 minutos de inatividade e nenhuma atividade de sessão ser relatada.

Sessões de aplicativos sem agente

O início e o fim da sessão para aplicativos sem agente são definidos da seguinte forma:

- Início: Você inicia o aplicativo a partir do aplicativo Citrix Workspace ou de um navegador da web.
- Fim: Uma sessão termina após 120 minutos de inatividade.

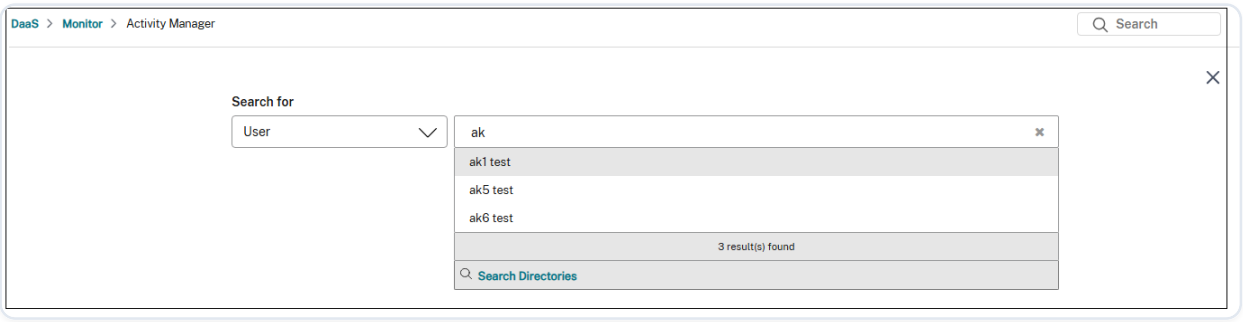
> **Limitação conhecida:**
>
> As sessões de aplicativos sem agente são encerradas após 120 minutos de inatividade, independentemente das configurações de tempo limite configuradas no console do Secure Private Access (**Configurações > Tempos Limite**).

Visualizar uma sessão do Secure Private Access por usuário

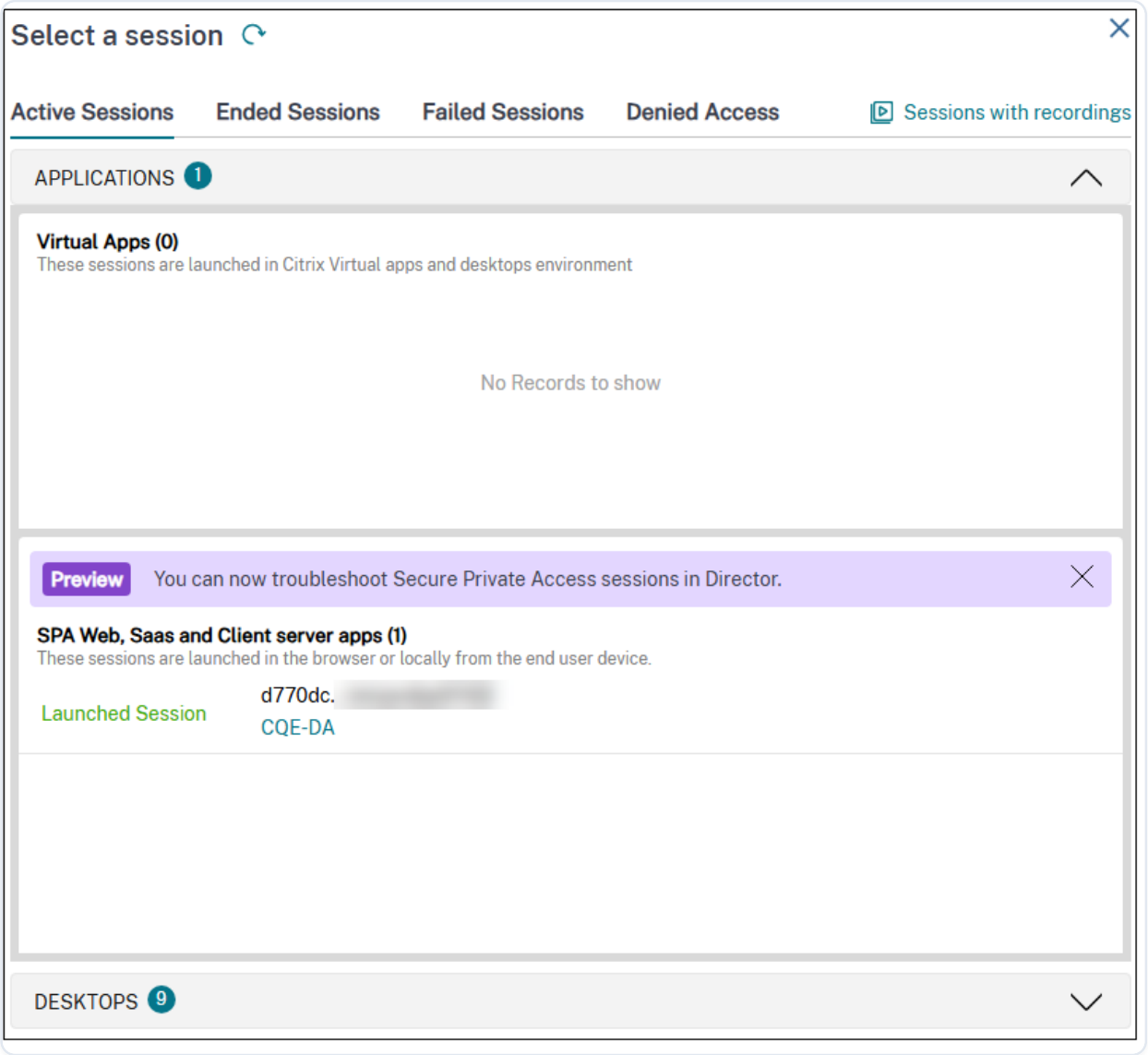
Visualizar uma sessão usando o campo Pesquisar

1. No painel do Monitor, clique em **Pesquisar** e insira o nome de usuário. A tela **Selecionar uma sessão** é exibida.

. Se você não encontrar o nome de usuário inserido, clique em **Pesquisar Diretórios** para encontrar o nome de usuário.

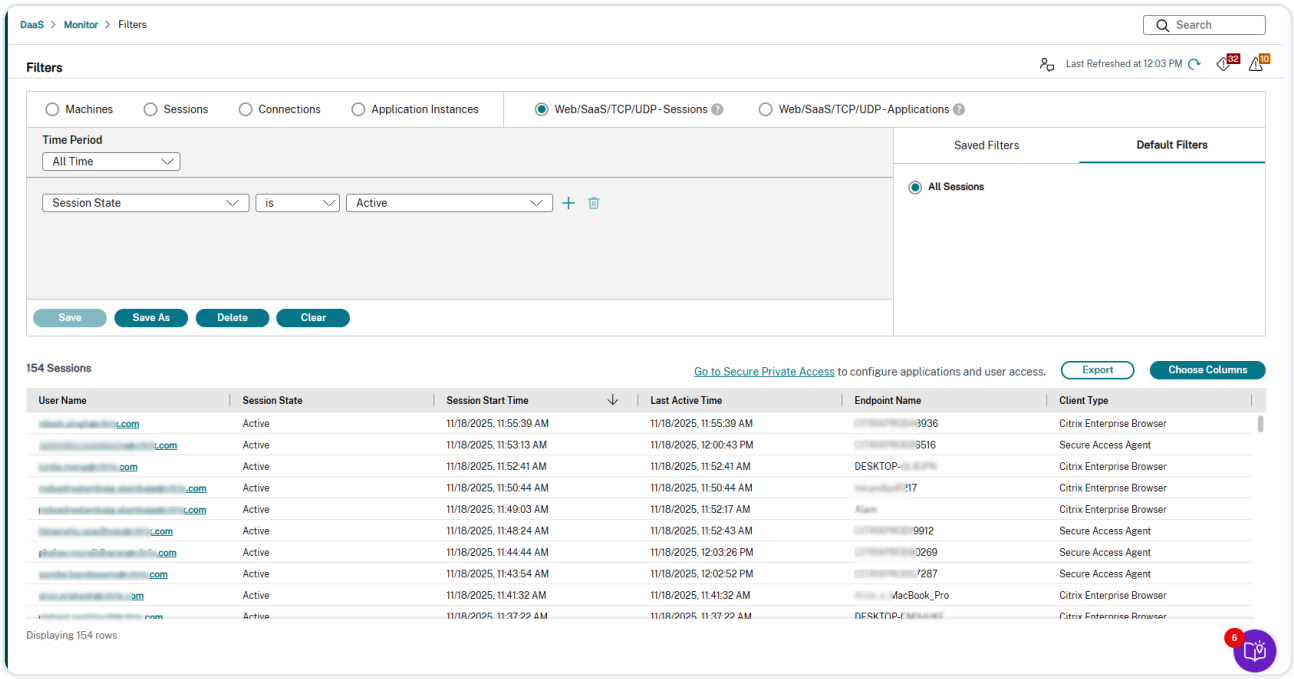


2. Selecione o usuário desejado. A tela **Selecionar uma sessão** é exibida.



Visualizar uma sessão na página Filtros

Você pode pesquisar as sessões na página **Filtros**, onde pode pesquisar sessões específicas usando as várias condições.



Execute as seguintes etapas para visualizar uma sessão de usuário na página **Filtros**:

- Refine sua pesquisa com base nos vários filtros, como máquinas, sessões, conexões, instâncias de aplicativos, sessões do Secure Private Access e aplicativos do Secure Private Access. Você também pode refinar sua pesquisa com base na linha do tempo.
- Use as listas suspensas para selecionar mais critérios de filtro (por exemplo, **Usuário associado**, **IP do endpoint** e assim por diante). Para obter mais informações, consulte Filtrar dados para solucionar falhas.

A lista de sessões associadas ao usuário especificado é exibida.

Gerenciador de Atividades para sessão do Secure Private Access

O Citrix Monitor oferece a visualização do Gerenciador de Atividades para sessões do Secure Private Access, que fornece uma visão geral das atividades da sessão. O Gerenciador de Atividades oferece uma visão abrangente de todos os aplicativos e desktops que foram abertos com sucesso, falharam ao abrir e o resultado das políticas definidas no aplicativo Secure Private Access.

O Gerenciador de Atividades contém as seguintes guias:

Aplicativos Disponíveis: Exibe os aplicativos que estão disponíveis no aplicativo Citrix Workspace. Esta seção mostra a última tentativa de enumeração dos aplicativos e o status da tentativa de enumeração.

Aplicativos Iniciados: Exibe os aplicativos que são abertos no aplicativo Citrix Workspace.

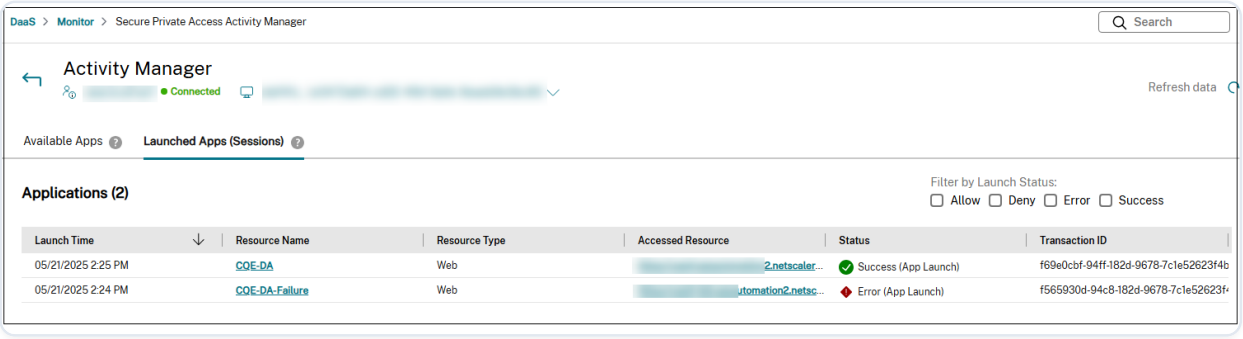
> **Nota:**
>
> Se um aplicativo for acessado várias vezes na mesma sessão, apenas os detalhes do acesso mais recente serão capturados.

Visualizar Gerenciador de Atividades

Para visualizar o Gerenciador de Atividades, faça o seguinte:

1. No painel do Monitor, clique em **Pesquisar** e insira o nome de usuário.

   . Se você não encontrar o nome de usuário inserido, clique em **Pesquisar Diretórios** para encontrar o nome de usuário.
2. Selecione o usuário desejado. A tela **Selecionar uma sessão** é exibida.
3. Selecione uma sessão ativa que foi aberta usando a sessão do Secure Private Access. O Gerenciador de Atividades para a sessão selecionada é exibido.



4. Clique em **Aplicativos Disponíveis** para visualizar os aplicativos que estão disponíveis no aplicativo Citrix Workspace ou clique em **Aplicativos Iniciados (sessões)** para visualizar os aplicativos que estão abertos no aplicativo Citrix Workspace.

   Você pode categorizar e filtrar recursos com base no status de acesso para os usuários. Esses status refletem o resultado das políticas configuradas no aplicativo Secure Private Access.

   - **Permitir:** Indica que a política do Secure Private Access permite o acesso ao recurso especificado. Como resultado, o recurso fica visível e acessível no aplicativo Citrix Workspace do usuário.
   - **Negar:** Indica que a política do Secure Private Access impede o acesso do usuário ao recurso. Embora o recurso possa estar visível no aplicativo Citrix Workspace do usuário, ele permanece inacessível, indicando restrições de acesso resultantes da aplicação da política.

- **Erro:** Indica um cenário em que um usuário deveria ter acesso a um recurso de acordo com as políticas do aplicativo Secure Private Access. No entanto, devido a um problema subjacente, o recurso não está funcionando corretamente ou está indisponível no aplicativo Citrix Workspace. O erro pode estar relacionado à enumeração ou à sessão.
- **Sucesso:** Indica se o lançamento do aplicativo foi bem-sucedido.

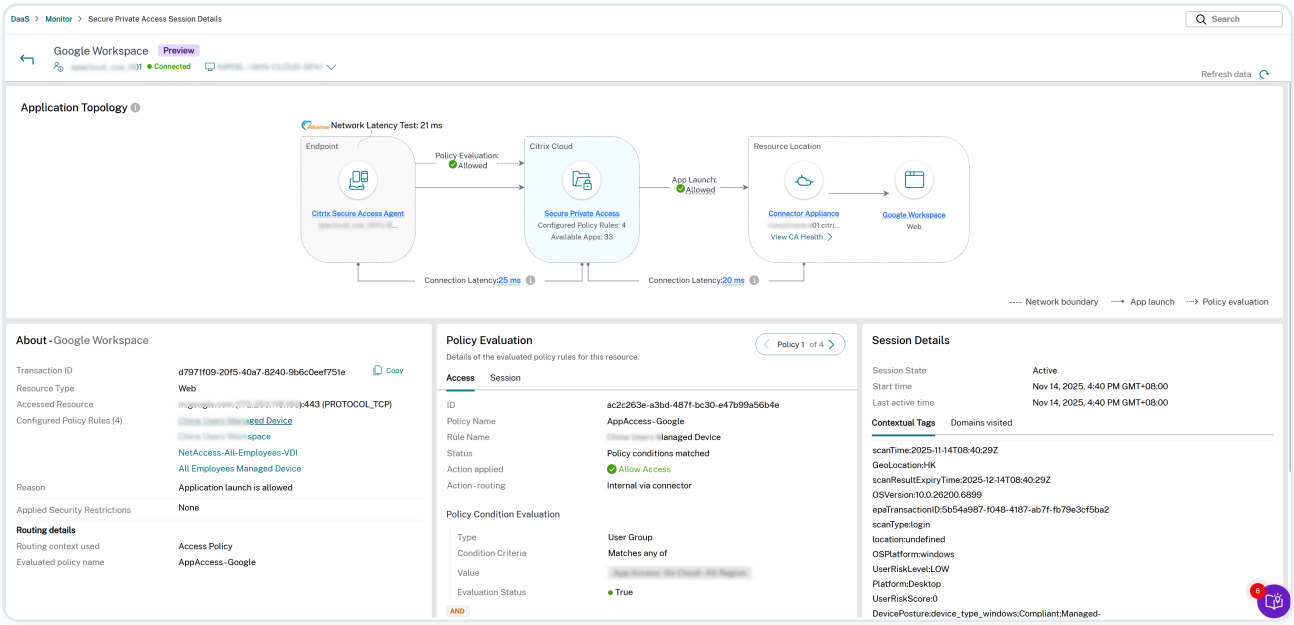
Página de Detalhes da Sessão do Secure Private Access

Uma página de Detalhes da Sessão do Secure Private Access contém os quatro painéis a seguir:

- **Topologia do aplicativo:** Fornece o fluxo do processo de inicialização do aplicativo. Além disso, fornece detalhes completos sobre o aplicativo. O endpoint se conecta ao Citrix Gateway e o Citrix Gateway se conecta ao plug-in do Secure Private Access. Usando as informações do plug-in do Secure Private Access, o aplicativo é iniciado.

  Você pode visualizar a topologia do aplicativo de um aplicativo na seção **Aplicativos disponíveis** ou **Aplicativos iniciados** do Gerenciador de Atividades. Você também pode visualizar a topologia do aplicativo para os aplicativos cujo acesso foi negado na guia **Acesso Negado**.
- **Detalhes do ponto de extremidade:** Exibe informações importantes sobre o dispositivo cliente e a rede usados para acessar o aplicativo. Passe o mouse sobre Ponto de extremidade para visualizar informações detalhadas.
- **Sobre:** Exibe informações adicionais sobre os aplicativos Web/SaaS, TCP/UDP e sem agente, tanto para os aplicativos iniciados com sucesso quanto para os aplicativos com falha.
- **Avaliação da Política:** Exibe informações relacionadas à política, como regras, ações e condições nas guias **Acesso** e **Sessão**.
  - Os detalhes da política de acesso podem ser visualizados na guia **Acesso**.
  - Os detalhes da política de sessão podem ser visualizados na guia **Sessão**.
- **Detalhes da Sessão:** Exibe os detalhes da sessão para uma sessão estabelecida com sucesso. Para uma sessão com falha, o motivo da falha da sessão é exibido.
- **Latência salto a salto:** Exibe os detalhes da latência para cada salto na topologia do aplicativo, incluindo o salto do Connector Appliance para o aplicativo de back-end. Ajuda os administradores a triar e isolar problemas de desempenho ou lentidão em vários saltos.

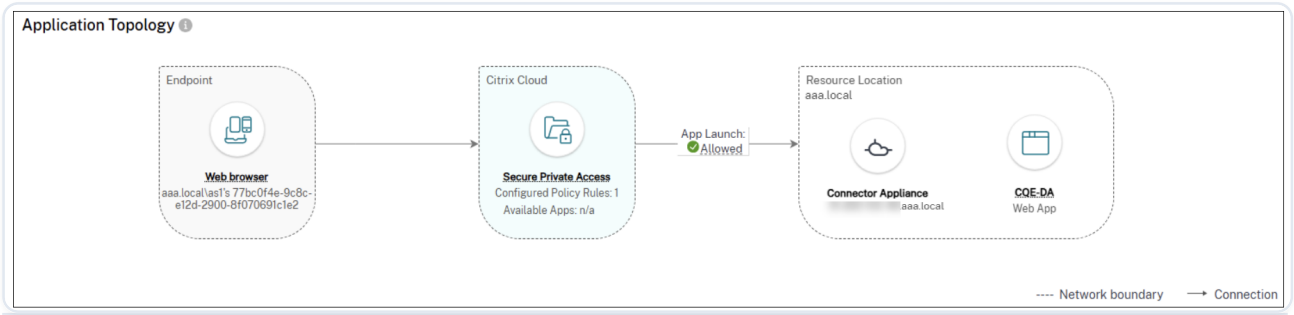
A figura a seguir exibe uma página de Detalhes da Sessão do Secure Private Access de exemplo para um lançamento de aplicativo bem-sucedido.



Topologia do aplicativo

Em um cenário de lançamento de aplicativo bem-sucedido, a Topologia do Aplicativo representa todo o fluxo de comunicação em uma cor uniforme. Por outro lado, quando um lançamento de aplicativo falha devido a problemas como um Connector Appliance inacessível ou um servidor de back-end indisponível, a Topologia do Aplicativo exibe o segmento específico do fluxo onde a falha ocorre em uma cor diferente. Por exemplo, se o Connector Appliance estiver inacessível, a conexão entre o Citrix Cloud™ e o Local de Recurso pode ser destacada em vermelho, indicando a falha. Para sessões do Chrome Enterprise Premium, a topologia também reflete a rota do aplicativo (`internal`, `external` ou `external_fixed_ip`) usada para o aplicativo lançado. Para o mapeamento entre esses termos e o campo **Roteamento de ação** na página Detalhes da Sessão, consulte Vocabulário de rota do aplicativo.

As figuras a seguir exibem um fluxo de aplicativo de exemplo.



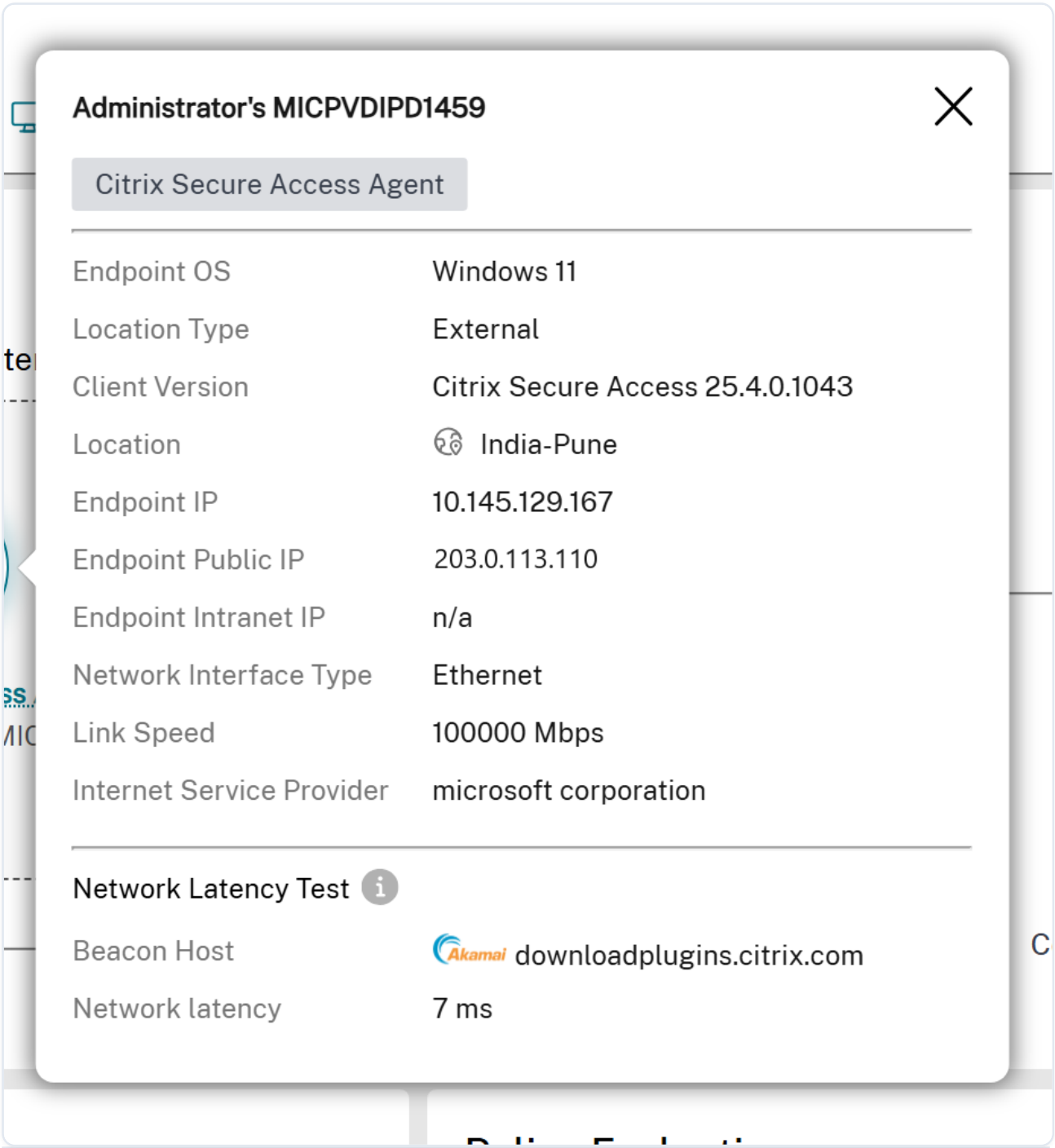
NOME DO CAMPO	DESCRIÇÃO
Ponto de extremidade	Exibe o ponto de extremidade onde o aplicativo é aberto. As opções possíveis são Citrix Workspace app e Citrix Secure Agent. O ID do dispositivo é exibido. Você também pode

NOME DO CAMPO	DESCRIÇÃO
	visualizar o SO do ponto de extremidade, IP do ponto de extremidade, tipo de local, local e detalhes da rede.
Citrix Cloud	Exibe o número de aplicativos enumerados e o número de políticas configuradas.
Avaliação da política	Exibe o resultado da política definida no aplicativo Secure Private Access. Os valores possíveis são **Permitido**, **Negado**, **Acesso permitido com restrições** e **Erro**.
Rede pública	Exibe o tipo de aplicativos e o status do lançamento do aplicativo. O valor possível para tipos de aplicativos é aplicativo Web/ SaaS. Da mesma forma, os valores possíveis para status de lançamento de aplicativos são **Permitido**, **Negado**, **Acesso permitido com restrições** e **Erro**. Você também pode visualizar a URL de nível superior, o tipo de aplicativo e a publicação do aplicativo.
Local do Recurso	Exibe o tipo de aplicativos e o status do lançamento do aplicativo. O valor possível para tipos de aplicativos é aplicativo TCP/UDP. Você também pode visualizar a URL de nível superior, o tipo de aplicativo e a publicação do aplicativo.

Detalhes do endpoint

Exibe informações importantes sobre o dispositivo cliente e a rede usados para acessar o aplicativo. Passe o mouse sobre Endpoint para ver informações detalhadas.

A figura a seguir exibe um painel de exemplo de **Detalhes do endpoint**.



NOME DO CAMPO	DESCRIÇÃO
SO do endpoint	O sistema operacional do dispositivo endpoint.
Tipo de local	O tipo de local de onde o dispositivo de endpoint está se conectando. Os valores possíveis são Interno e Externo.
Versão do Cliente	A versão do aplicativo Citrix Workspace ou do cliente Citrix Secure Access instalado no dispositivo de endpoint.

NOME DO CAMPO	DESCRIÇÃO
Localização	A localização geográfica do dispositivo de endpoint com base em seu endereço IP.
IP do Endpoint	O endereço IP privado do dispositivo de endpoint.
IP Público do Endpoint	O endereço IP público do dispositivo de endpoint.
IP da Intranet do Endpoint	O endereço IP da intranet do dispositivo de endpoint.
Tipo de Interface de Rede	O tipo de interface de rede usada pelo dispositivo de endpoint. Os valores possíveis são Ethernet, Wi-Fi, Celular e Outro.
Força do Sinal	A força do sinal da conexão de rede no dispositivo de endpoint, medida em dBm.
Velocidade do Link	A velocidade da conexão de rede no dispositivo de endpoint, medida em Mbps.
Provedor de Serviços de Internet	O nome do Provedor de Serviços de Internet (ISP) para o dispositivo de endpoint.
Host do Beacon	O nome do host do servidor beacon usado para verificações de conectividade.
Latência da Rede	O tempo de ida e volta para os pacotes de dados viajarem do dispositivo de endpoint para o servidor beacon e vice-versa, medido em milissegundos (ms).

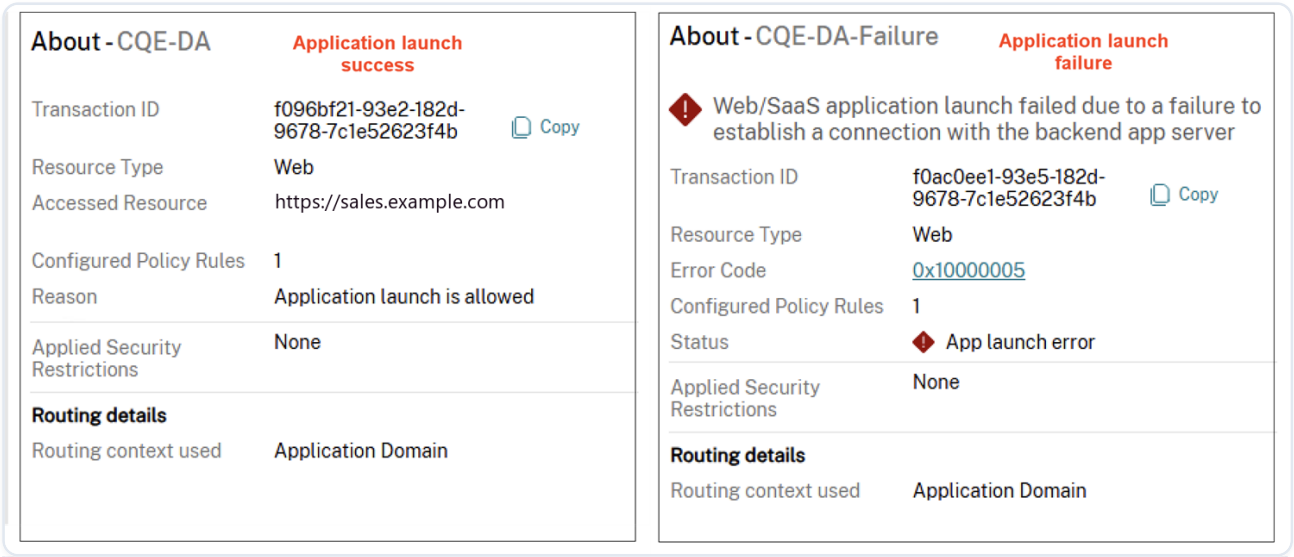
Esta informação ajuda os administradores a identificar o caminho da rede, solucionar problemas de conectividade e correlacionar o desempenho com endpoints específicos. Os campos são exibidos com base no tipo de implantação e nos dados disponíveis.

Painel Sobre

Exibe informações adicionais sobre os aplicativos Web/SaaS, TCP/UDP e sem agente, tanto para os aplicativos iniciados com sucesso quanto para os aplicativos com falha. Nos casos em que um

aplicativo falha, o painel **Sobre** mostra o código de erro correspondente. Clicar neste código redireciona você para uma página de documentação que detalha a causa e a solução alternativa. Para outros problemas, você é direcionado para a página de suporte da Citrix.

A figura a seguir exibe um exemplo do painel **Sobre**.

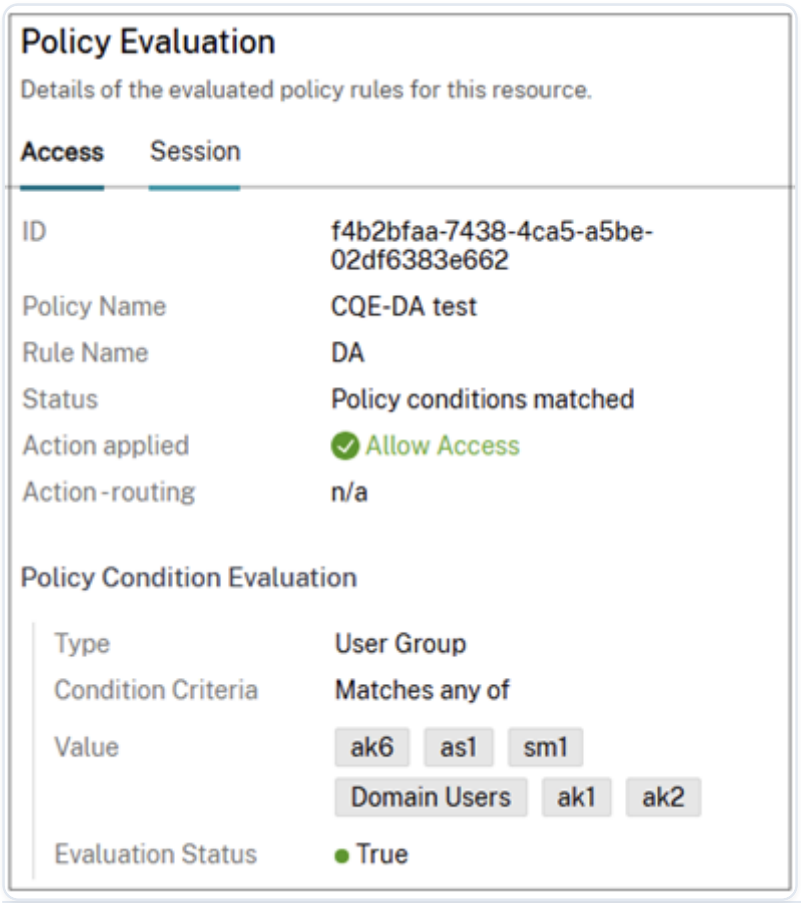


NOME DO CAMPO	DESCRIÇÃO
ID da Transação	ID da Transação Citrix gerado durante a sessão ou enumeração.
Tipo de Recurso	Exibe o tipo de recurso. Os valores possíveis são Web, SaaS, TCP/UDP (Servidor para Cliente) e TCP/UDP (Cliente para Servidor).
Recursos Acessados	Os dados que aparecem no campo **Recursos Acessados** variam dependendo do tipo de aplicativo.
	Aplicativos SaaS - URL ou o FQDN do aplicativo
	TCP/UDP – Endereço IP/FQDN, porta e protocolo
	Aplicativo Web (iniciado via cliente Citrix Secure Access) - FQDN, porta e protocolo
	Aplicativo Web (iniciado via Citrix Workspace) - URL

NOME DO CAMPO	DESCRIÇÃO
	Aplicativos sem agente - URL do aplicativo
Regras de Política Configuradas	O número de políticas que são usadas em uma sessão ou enumeração.
Motivo	O resultado da análise da atividade da sessão ou enumeração.
Restrições de segurança aplicadas	Exibe as restrições de segurança que são aplicadas a este aplicativo.
Contexto de roteamento	Exibe o tipo de política (política de acesso, política de sessão ou domínio do aplicativo) aplicada durante o roteamento. O contexto de roteamento ajuda a identificar a hierarquia (política de acesso > política de sessão > domínio de aplicativo padrão) que influencia as decisões de roteamento.
	Para a política de sessão, o link Ver detalhes fornece detalhes adicionais sobre a política de sessão.

Painel de Avaliação de Política

Exibe informações relacionadas à política, como regras, ações e condições nas guias **Acesso** e **Sessão**. Os detalhes da política de acesso podem ser visualizados na guia **Acesso**. Os detalhes da política de sessão podem ser visualizados na guia **Sessão**.



NOME DO CAMPO	DESCRIÇÃO
ID	ID de transação Citrix
Nome da Política	O nome da política associada ao aplicativo. Se houver várias políticas, a primeira política que corresponder à condição definida aparecerá.
Nome da regra	O nome da regra configurado dentro da política.
Status	Resultados da avaliação da política
Ação aplicada	A ação aplicada ao aplicativo com base nos resultados da avaliação da política. Por exemplo, negar acesso.
Roteamento de ação	Exibe o caminho de roteamento (Direto, Interno via conector, Interno via gateway) que a solicitação de um usuário percorre através do serviço Secure Private Access. Para o mapeamento entre esses valores e os termos do diagrama usados na topologia do Chrome

NOME DO CAMPO	DESCRIÇÃO
	Enterprise Premium, consulte Vocabulário de rota de aplicativo.
Tipo	O tipo da condição da política.
Critérios da Condição	Os critérios da condição da política aplicada na sessão ou durante a enumeração.
Valor	Resultados da avaliação da condição.
Status da avaliação	Status do resultado da avaliação da condição da política. Os diferentes valores são Permitido, Negado, Acesso permitido com restrições e Erro.

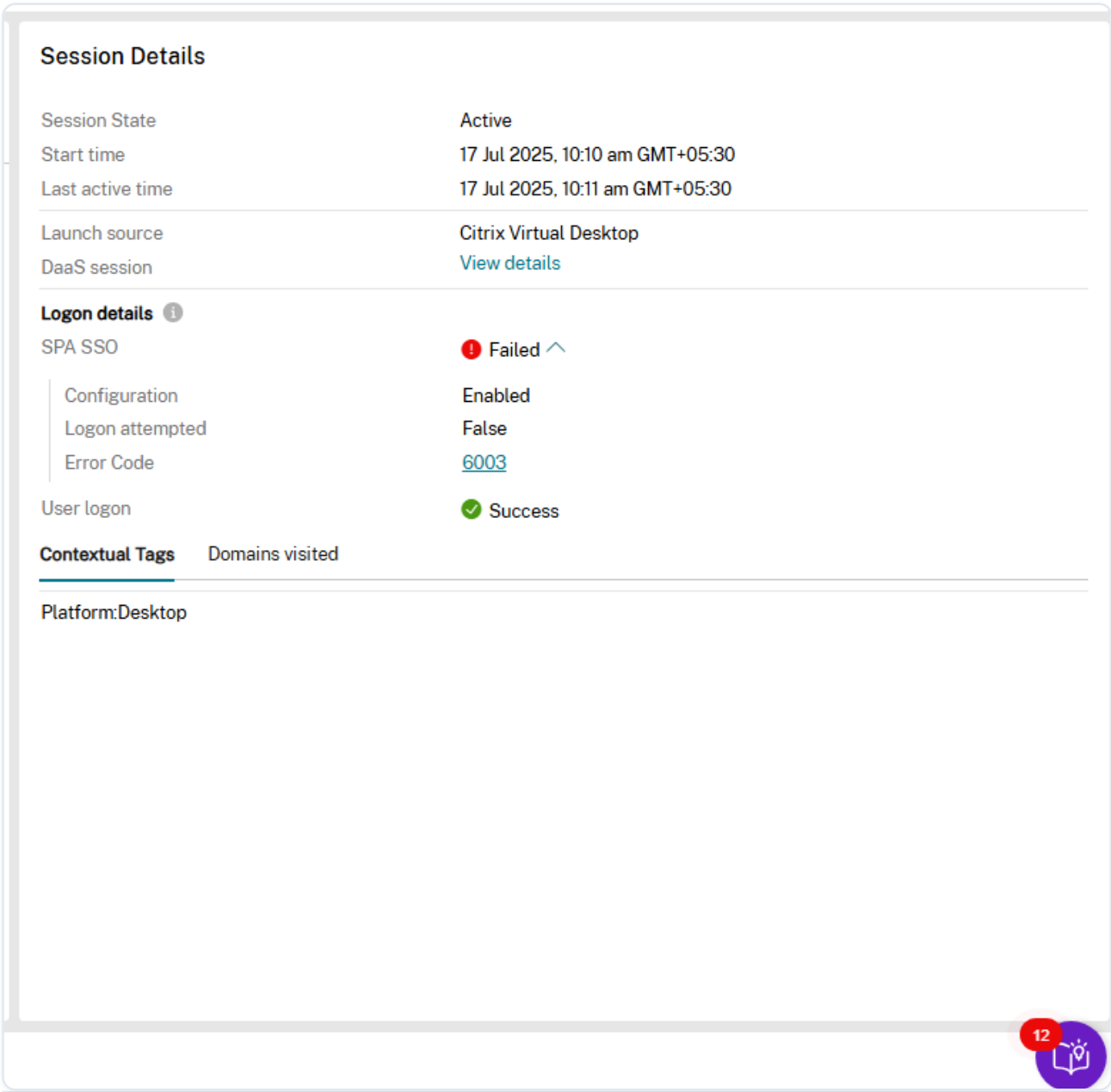
Nota:

Os campos **Nome do Aplicativo**, **Tipo de Aplicativo**, **Políticas** e **Controles de Segurança** podem exibir valores transferidos de um evento de enumeração quando o evento de inicialização do aplicativo original não inclui esses valores. O campo **Caminho de dados** também pode aparecer vazio quando o evento de origem não o especifica.

Painel Detalhes da Sessão

Para uma sessão com falha, o motivo da falha da sessão é exibido. Para uma sessão bem-sucedida, detalhes adicionais relacionados à sessão são exibidos.

O painel **Detalhes da Sessão** permanece vazio para aplicativos clicados na guia **Aplicativos Disponíveis**, pois a enumeração de aplicativos não está associada a uma sessão.



NOME DO CAMPO	DESCRIÇÃO
Estado da sessão	Exibe o estado da sessão, seja ela ativa ou inativa.
Hora de início	Exibe a hora de início da sessão.
Última hora ativa	Exibe a última hora ativa da sessão bem-sucedida.
Origem do lançamento	Exibe a origem de onde a sessão do Secure Private Access é iniciada.

NOME DO CAMPO	DESCRIÇÃO
Sessão DaaS	Exibe os detalhes da sessão DaaS. Este campo aparece apenas no caso de um VDA de sessão única ou multi-sessão.
Detalhes de logon	
SSO SPA	Exibe se o logon único na sessão do Secure Private Access foi bem-sucedido ou falhou. Se falhou, o usuário deve fazer login manualmente.
Configuração	Exibe o status da configuração do logon único na sessão do Secure Private Access. Se não estiver configurado, os detalhes serão compartilhados com o administrador.
Tentativa de logon	Exibe o status da tentativa de logon de logon único para a sessão do Secure Private Access.
Código de erro	Exibe o código de erro quando a tentativa de logon único para a sessão do Secure Private Access falha. Os possíveis códigos de erro são: 6007 e 6003.
	6003- Erro ao recuperar o manipular de logon único do Secure Private Access do serviço Broker Agent.
	6007- Falha ao fazer login no Secure Private Access.
Logon do usuário	Exibe o status de logon manual do usuário para a sessão do Secure Private Access.
IP Virtual do Gateway	Exibe o endereço IP virtual do gateway ao qual a sessão bem-sucedida está conectada.
	Este campo é aplicável apenas para implantação de caminho de dados híbrido.

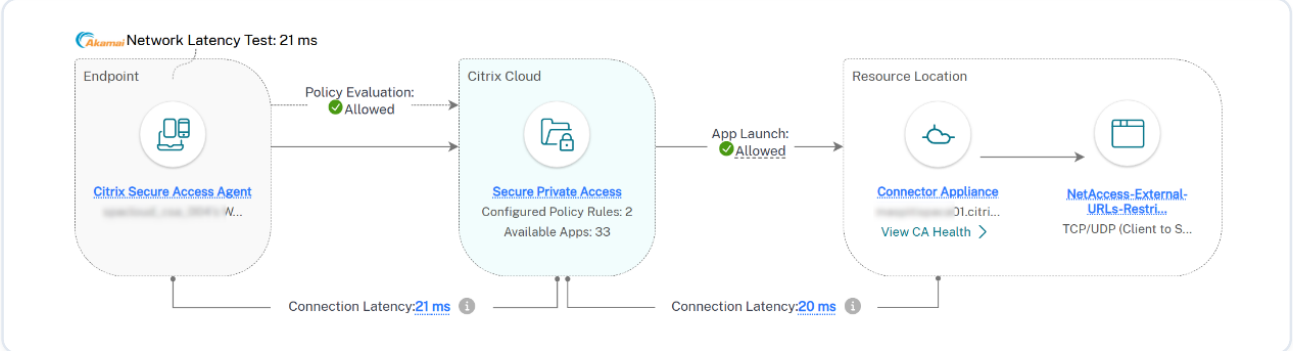
NOME DO CAMPO	DESCRIÇÃO
Tags Contextuais	Exibe as tags contextuais. A tag contextual no plug-in do Secure Private Access é o nome de uma política do NetScaler® Gateway (sessão, pré-autenticação, EPA) que é aplicada às sessões dos usuários autenticados.
Domínios visitados (Internos)	Exibe os domínios internos acessados usando a sessão bem-sucedida.
Domínios visitados (Externos)	Exibe os domínios externos acessados usando a sessão bem-sucedida.
	O campo **Domínios Visitados** é aplicável apenas para aplicativos Web/SaaS e é atualizado somente após 15 minutos, pois os clientes do Citrix Enterprise Browser no macOS e Windows enviam a atividade da sessão a cada 15 minutos.

Nota:

O painel da coluna Detalhes da Sessão permanece vazio para aplicativos clicados na guia Aplicativos Disponíveis, pois a enumeração de aplicativos não está associada a uma sessão.

Latência salto a salto

Os detalhes da latência para cada salto na topologia do aplicativo são exibidos em cada caminho. Esta informação ajuda os administradores a triar e isolar problemas de desempenho ou lentidão em vários saltos.

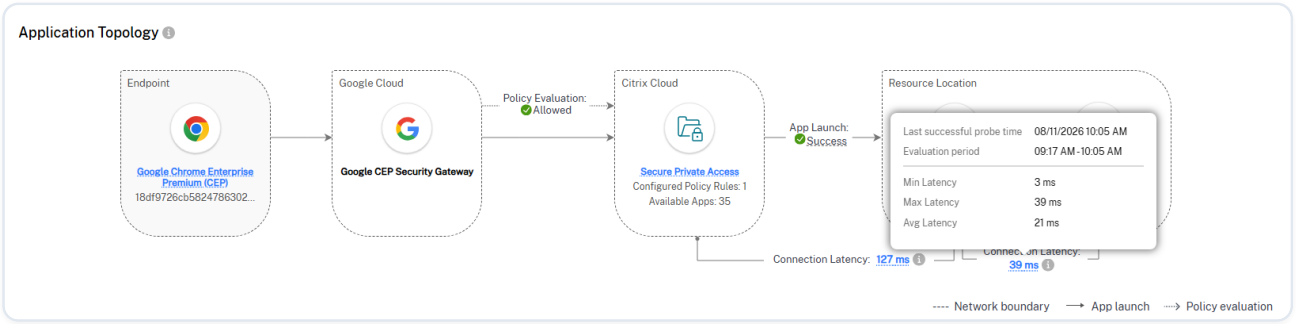


Nota:

- As informações de latência salto a salto estão disponíveis apenas para aplicativos iniciados via Secure Access Client versão V25.7.1.x ou posterior.
- As informações de latência do cliente para o SPA são exibidas apenas para a última hora. Se a sessão não esteve ativa na última hora, nenhum dado será exibido.

LATÊNCIA DO CONNECTOR APPLIANCE PARA O APLICATIVO DE BACKEND

Quando uma sessão do Secure Private Access atinge seu backend através de um Connector Appliance, a topologia mostra um rótulo de **Latência de Conexão** no link entre o Connector Appliance e o aplicativo de backend. Este valor é o tempo de ida e volta (RTT) entre o Connector Appliance e o backend, medido usando sondas sintéticas periódicas. Ele completa a visualização salto a salto, juntamente com a latência mostrada nos saltos anteriores. Como o Connector Appliance mede este salto diretamente, a leitura não depende da versão do cliente do endpoint.



O Connector Appliance registra quatro valores para este salto durante a janela de avaliação (a última hora):

- **Mínimo:** O RTT mais baixo medido na janela.
- **Máximo:** O RTT mais alto medido na janela.
- **Média:** O RTT médio na janela.
- **P90:** O RTT do percentil 90.

O rótulo da topologia exibe o valor P90.

O Connector Appliance envia sondas RTT a cada 15 minutos para os endereços IP de backend para os quais ele encaminhou tráfego nas últimas 8 horas. Se a sessão não teve atividade de backend na última hora, nenhum valor é exibido. O Monitor mantém esses dados de latência por 3 dias.

Atualmente, a latência do Connector Appliance para o aplicativo de backend aparece apenas para implantações em nuvem. Pode não aparecer para todas as sessões elegíveis ainda.

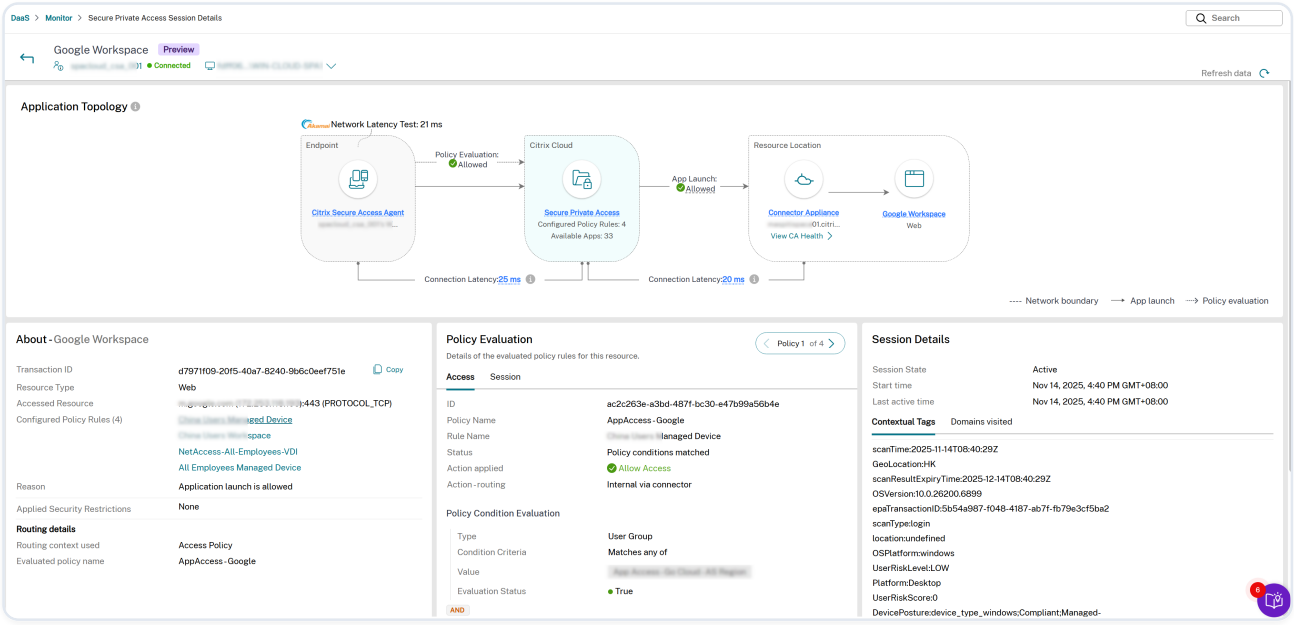
Ao passar o mouse sobre o rótulo, é exibida a seguinte dica de ferramenta: `Connection Latency is a synthetic metric (P90) measured over the evaluation window, collected periodically as probes between defined endpoints.`.

Nota:

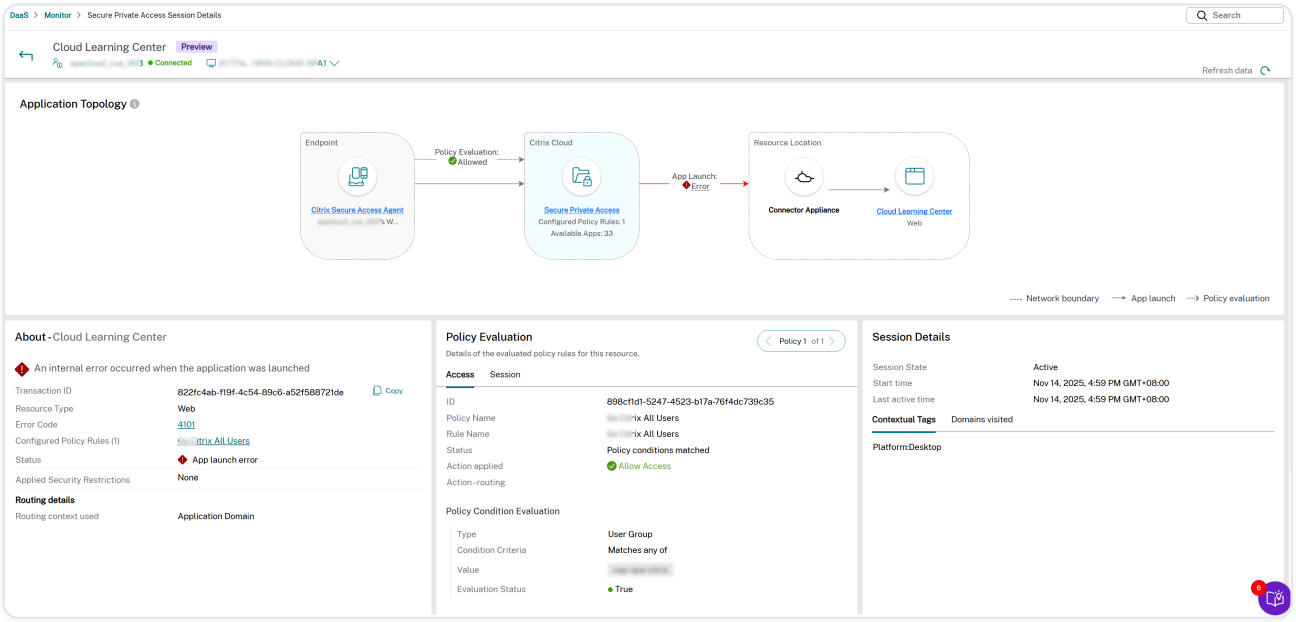
- Um valor de `-1` significa que o backend estava inacessível a partir do Connector Appliance durante a sonda.
- Um valor em branco ou **n/a** significa que nenhum dado de sonda foi coletado ainda para esse backend.
- Se este salto mostrar alta latência ou `-1`, execute uma sonda sob demanda do Connector Appliance para o backend para confirmar a acessibilidade e isolar o estágio com falha. Para obter mais informações, consulte Solucionar problemas de acessibilidade do aplicativo.

Exemplos de diagramas de topologia para os vários aplicativos

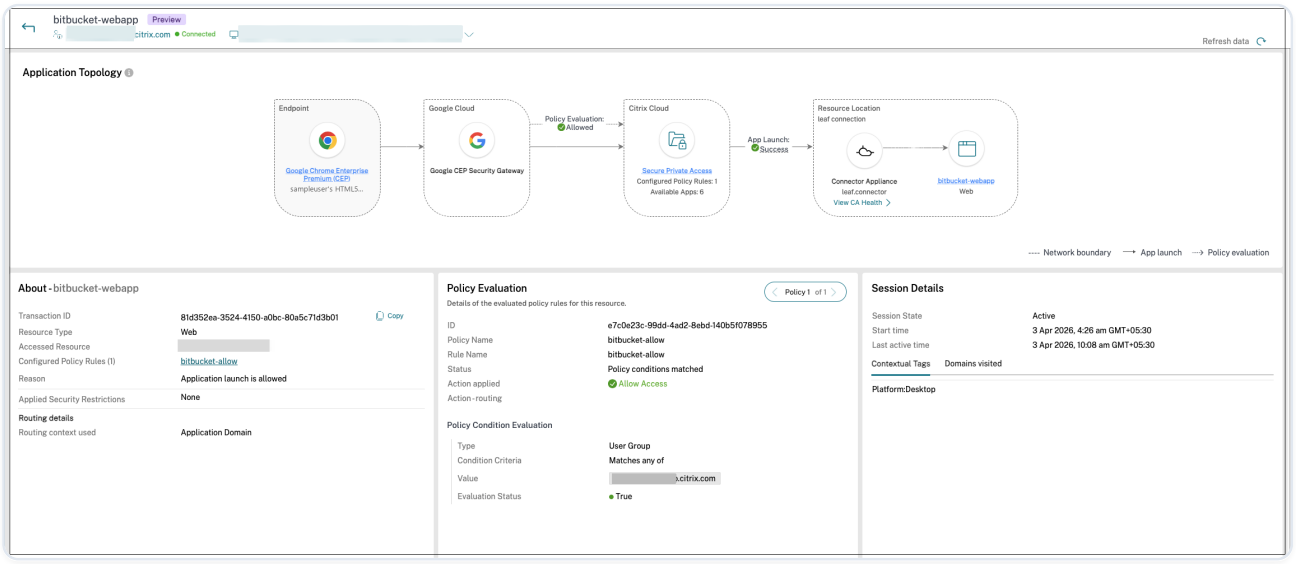
Aplicativos Web/SaaS - Cenário de sucesso:



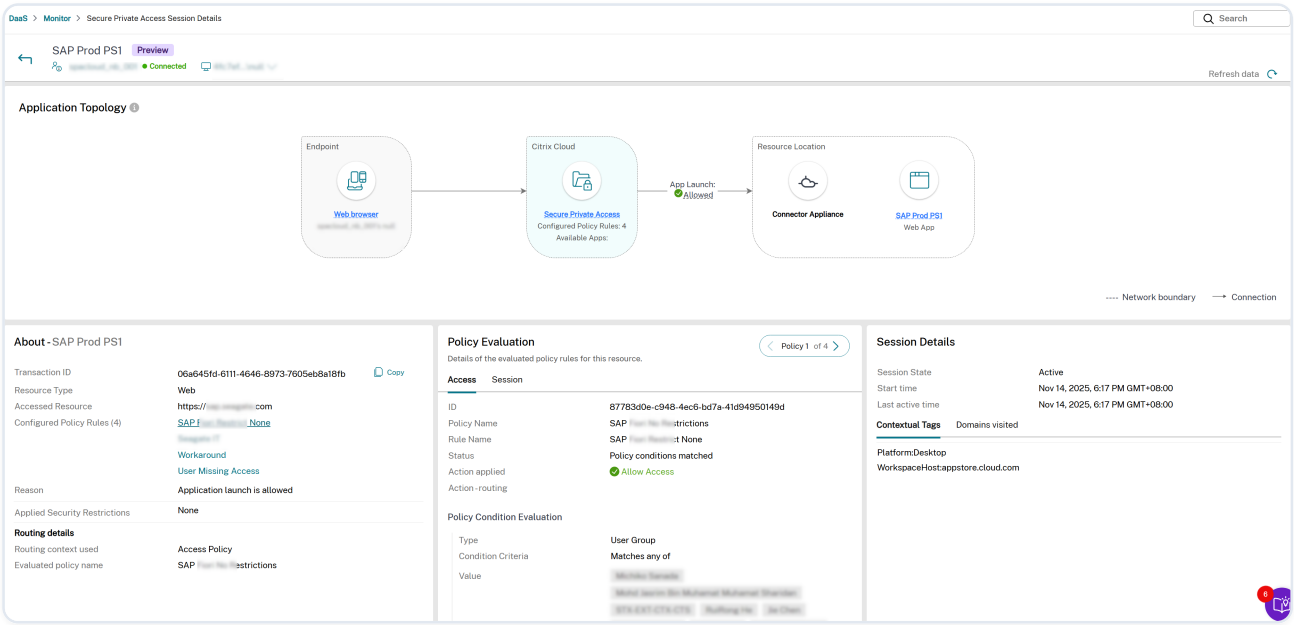
Aplicativos Web/SaaS - Cenário de falha:



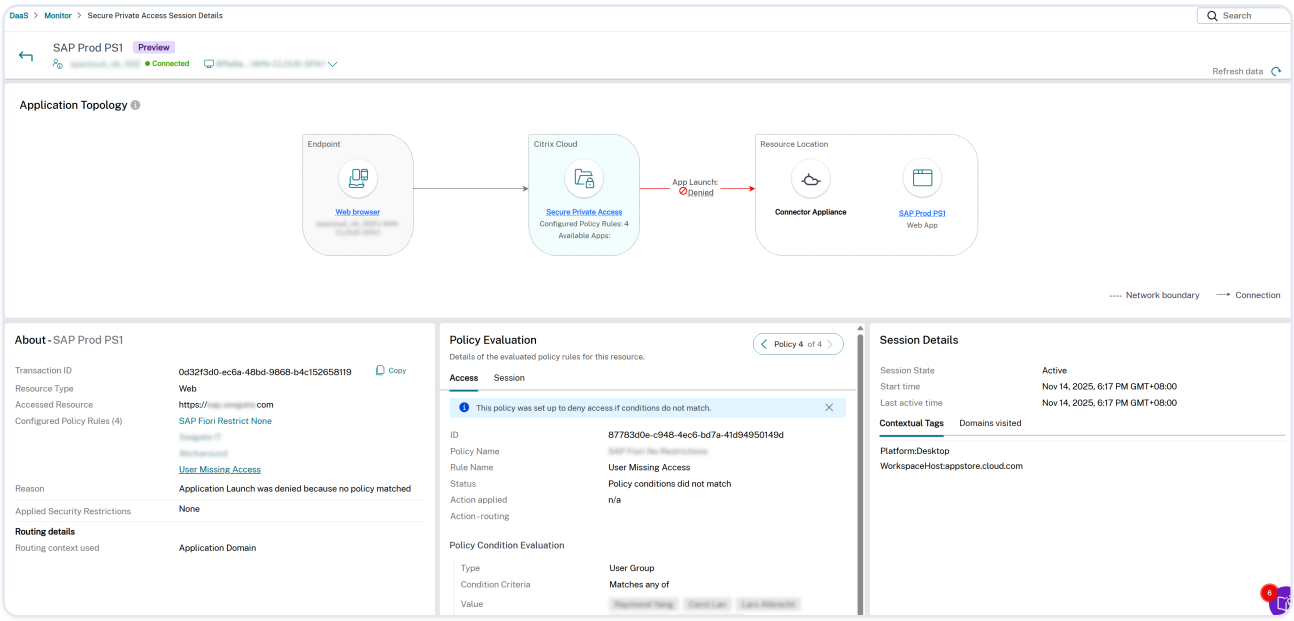
Tráfego de aplicativos SaaS roteado através do Google Secure Gateway:



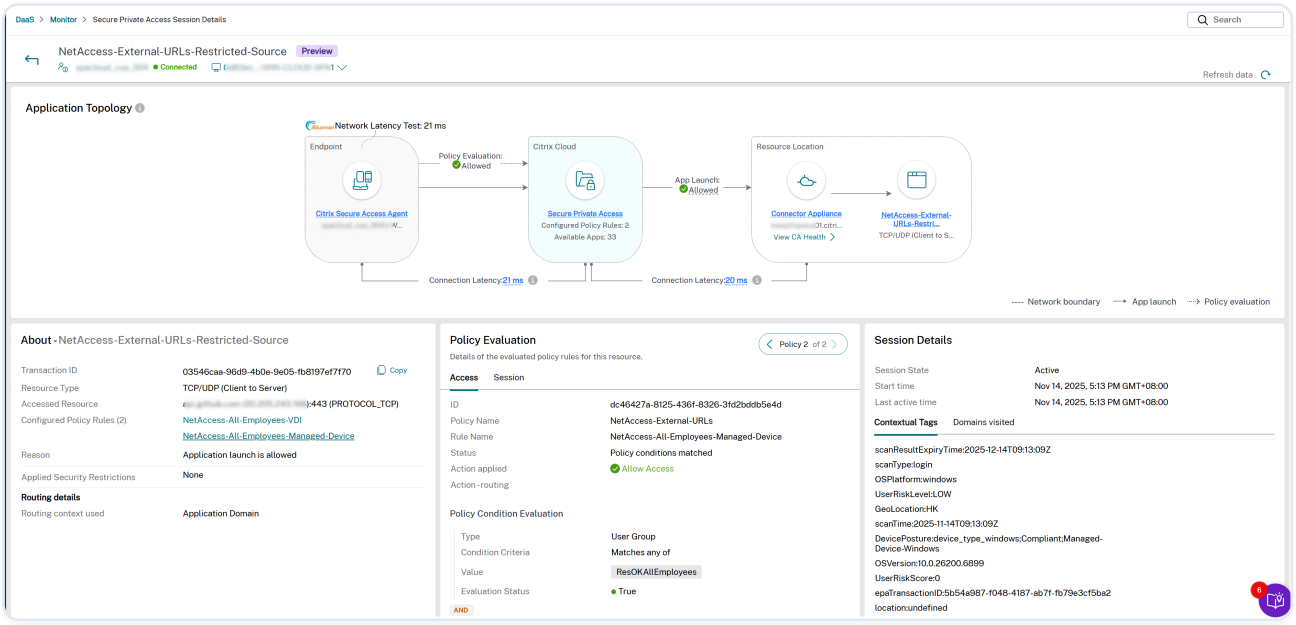
Aplicativos sem agente - cenário de sucesso:



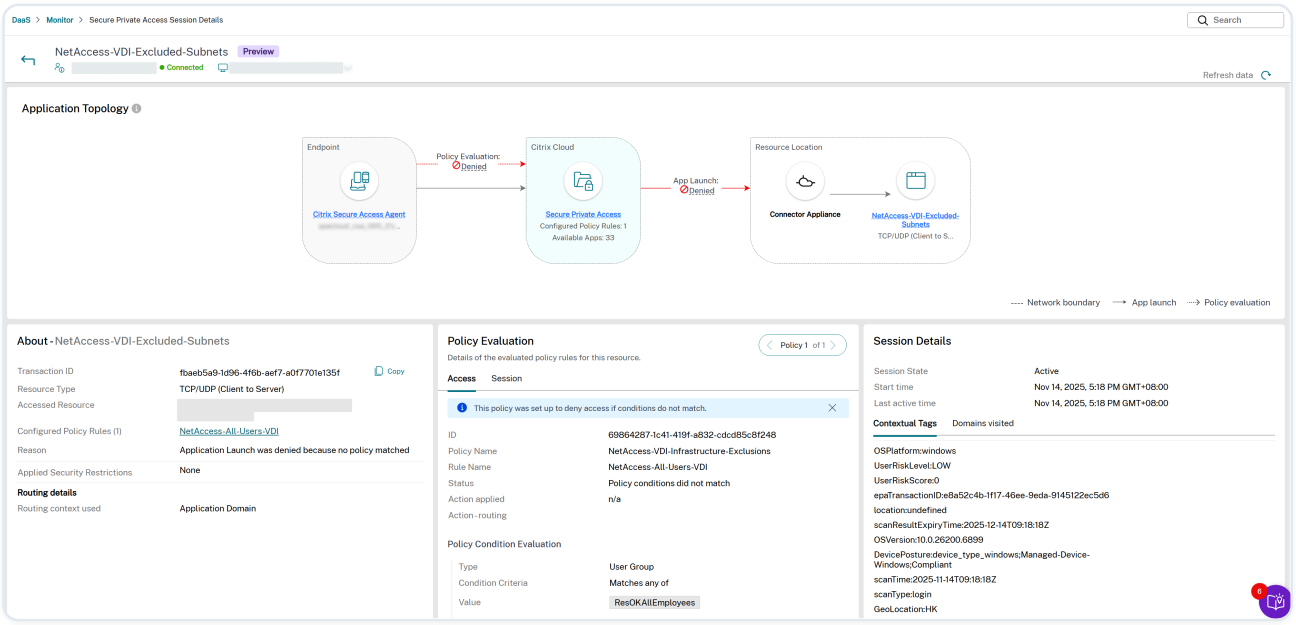
Aplicativos sem agente - Cenário de falha:



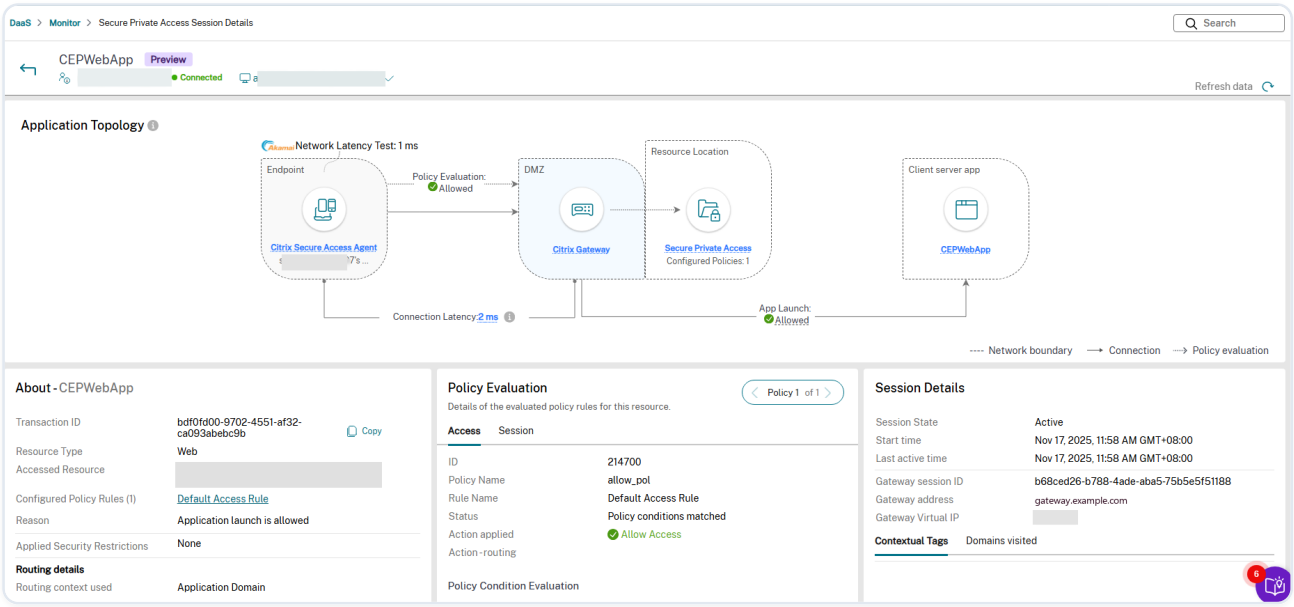
Aplicativos TCP/UDP - cenário de sucesso:



Aplicativos TCP/UDP - Cenário de falha:



Implantação híbrida:



Vocabulário de rota de aplicativo

Os diagramas de topologia do Chrome Enterprise Premium usam a taxonomia de `applicationRoute` de back-end, enquanto o campo **Roteamento de ação** na página Detalhes da sessão usa os rótulos de roteamento mostrados na interface do usuário do Monitor. A tabela a seguir mapeia os dois.

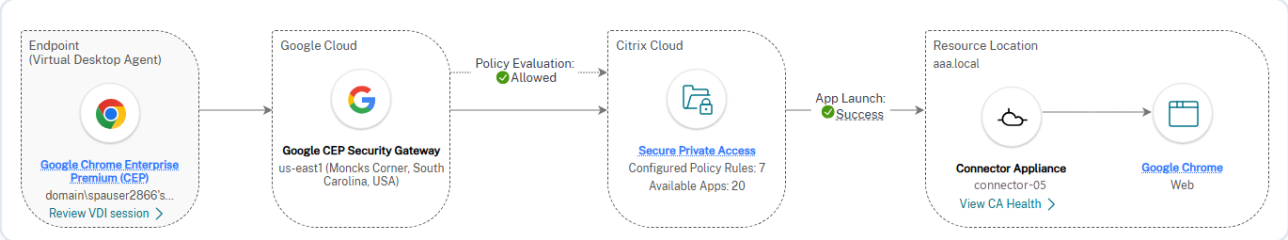
VOCABULÁRIO DO DIAGRAMA (`APPLICATIONROUTE`)	RÓTULO DA INTERFACE DO USUÁRIO DE ROTEAMENTO DE AÇÃO	SIGNIFICADO
`internal`	Interno via conector	O tráfego sai por um Connector Appliance no local do recurso.
`external`	Direto	O tráfego sai diretamente para o aplicativo de back-end, sem atravessar a saída de IP fixo do Secure Private Access.
`external_fixed_ip`	Interno via gateway	O tráfego sai pelo gateway do Secure Private Access com um IP de saída fixo para permitir a listagem no destino.

Variantes de topologia do Chrome Enterprise Premium

A topologia do Chrome Enterprise Premium possui seis variantes, determinadas pelo tipo de implantação (nuvem ou híbrida) e pela rota do aplicativo (`internal`, `external` ou `external_fixed_ip`) para o aplicativo iniciado. Uma inicialização com falha destaca o segmento com falha do fluxo em uma cor diferente, conforme descrito em Topologia do aplicativo. Para as etapas de triagem de acessibilidade do aplicativo, consulte Solucionar problemas de acessibilidade do aplicativo.

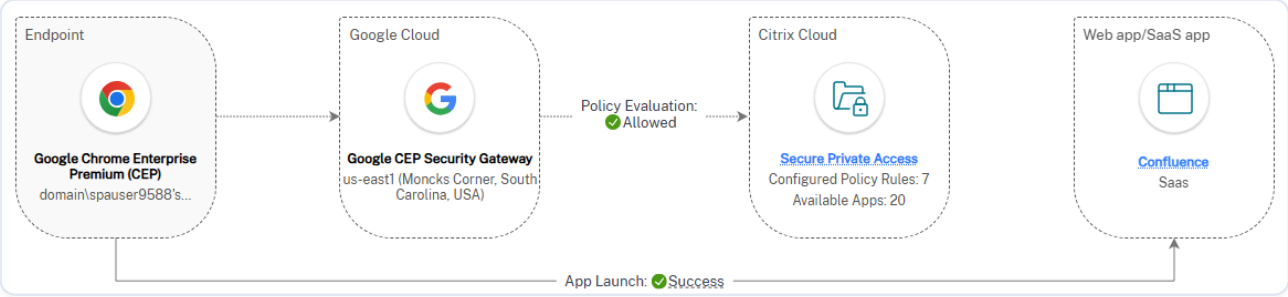
IMPLANTAÇÃO NA NUVEM — ROTA INTERNA

Uma sessão do Chrome Enterprise Premium em uma implantação na nuvem usa a rota interna quando o aplicativo de destino é acessado por meio de um Connector Appliance no local do recurso. O tráfego flui do endpoint do Chrome Enterprise Premium através do Citrix Cloud para o Connector Appliance e, em seguida, para o aplicativo de back-end interno.



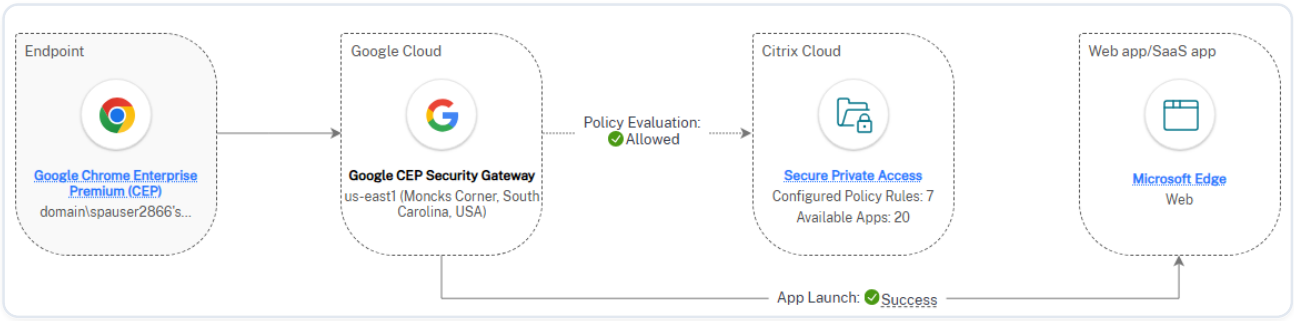
IMPLANTAÇÃO NA NUVEM — ROTA EXTERNA

Uma sessão do Chrome Enterprise Premium em uma implantação na nuvem usa a rota externa quando o aplicativo de destino é acessado diretamente, sem atravessar a saída de IP fixo do Secure Private Access. O tráfego flui do endpoint do Chrome Enterprise Premium através do Citrix Cloud diretamente para o aplicativo de back-end externo.



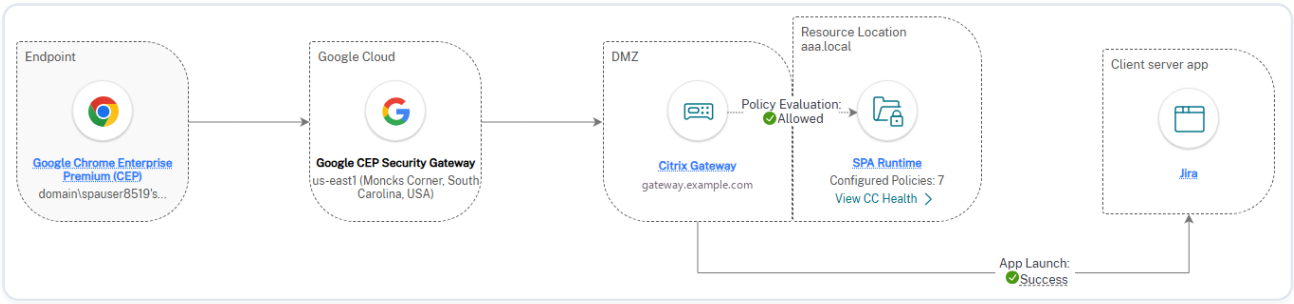
IMPLANTAÇÃO NA NUVEM — ROTA DE IP FIXO EXTERNA

Uma sessão do Chrome Enterprise Premium em uma implantação na nuvem usa a rota de IP fixo externa quando o destino requer um IP de saída conhecido para a lista de permissões. O tráfego flui do endpoint do Chrome Enterprise Premium através do Citrix Cloud e da saída de IP fixo do Secure Private Access para o aplicativo de back-end externo.



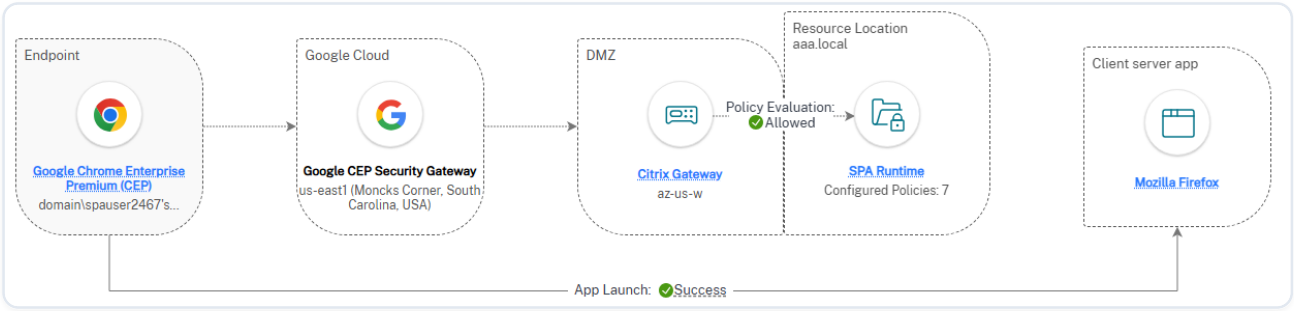
IMPLANTAÇÃO HÍBRIDA — ROTA INTERNA

Uma sessão do Chrome Enterprise Premium em uma implantação híbrida usa a rota interna quando o aplicativo de destino é acessado por meio de um Connector Appliance no local do recurso. O tráfego flui do endpoint do Chrome Enterprise Premium através do Citrix Gateway local para o Connector Appliance e, em seguida, para o aplicativo de back-end interno.



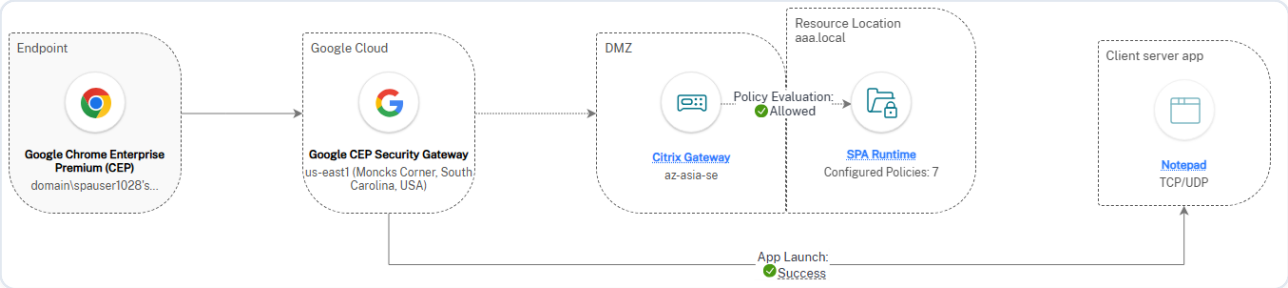
IMPLANTAÇÃO HÍBRIDA — ROTA EXTERNA

Uma sessão do Chrome Enterprise Premium em uma implantação híbrida usa a rota externa quando o aplicativo de destino é acessado diretamente, sem atravessar a saída de IP fixo do Secure Private Access. O tráfego flui do endpoint do Chrome Enterprise Premium através do Citrix Gateway local diretamente para o aplicativo de back-end externo.



IMPLANTAÇÃO HÍBRIDA — ROTA DE IP FIXO EXTERNA

Uma sessão do Chrome Enterprise Premium em uma implantação híbrida usa a rota de IP fixo externa quando o destino requer um IP de saída conhecido para a lista de permissões. O tráfego flui do endpoint do Chrome Enterprise Premium através do Citrix Gateway local e da saída de IP fixo do Secure Private Access para o aplicativo de back-end externo.



Criar e gerenciar alertas

Você pode configurar alertas para monitorar proativamente condições e escopos de seu interesse e reduzir a fadiga de alertas. Os alertas podem ser configurados com severidade, intervalos de re-alerta, meios de notificação e seguem o ciclo de vida de alerta suportado no produto.

Para obter mais informações, consulte o seguinte:

- Alertas
- Políticas de alerta avançadas

Suporte para Chrome Enterprise Premium

O Citrix Monitor oferece suporte ao Chrome Enterprise Premium (CEP) para Secure Private Access, permitindo monitoramento e solução de problemas abrangentes de sessões de aplicativos Web/SaaS iniciadas usando o Chrome Enterprise em todos os dispositivos.

Principais recursos:

- Pesquisa e filtragem de sessões de usuário: Pesquise e filtre sessões de usuário CEP em todos os dispositivos usando o filtro Tipo de Cliente na página Filtros.
- Revisão da atividade da sessão: Visualize a atividade da sessão, enumerações de perfil de usuário e inicializações de aplicativos para usuários CEP.
- Detalhes e topologia da sessão: Acesse o painel Detalhes da Sessão para revisar a topologia da transação de inicialização do aplicativo, incluindo componentes de back-end (SPA PoP, Connector Appliance e Cliente).
- Triagem de política de acesso: Analise os resultados da política de acesso, incluindo erros de negação, para sessões CEP.
- Visibilidade em toda a página Filtros: Visualize dados detalhados de sessão e aplicativo CEP, incluindo erros de inicialização, diretamente no fluxo de trabalho de topologia.
- Coleta de dados de domínio e inicialização: Colete e exiba dados sobre domínios visitados (acesso interno, externo, direto e marcado) e eventos de inicialização de aplicativos.

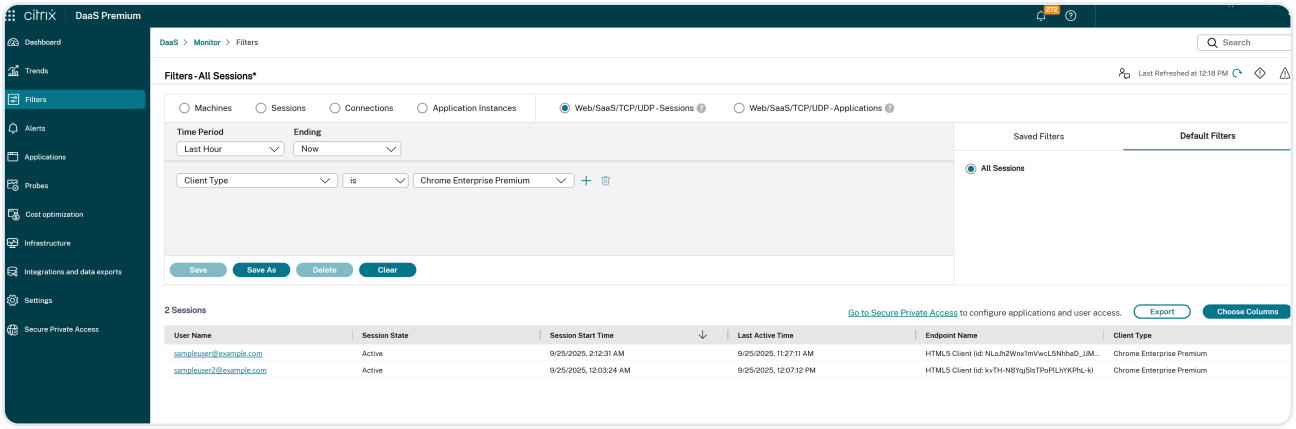
- Visibilidade do ciclo de vida da sessão: Monitore o ciclo de vida da sessão, batimentos cardíacos e eventos com até 7 dias de dados históricos.
- Paridade de dados: Garanta dados e visibilidade consistentes para todos os cenários de inicialização — aplicativo Citrix Workspace, CEP direto, SPA híbrido e implantações de nuvem SPA.

Nota:

Para monitorar e solucionar problemas de sessões de aplicativos Web/SaaS iniciadas usando o Chrome Enterprise, certifique-se de ter a licença Chrome Enterprise Premium. Para obter mais informações sobre o Chrome Enterprise Premium, consulte Chrome Enterprise.

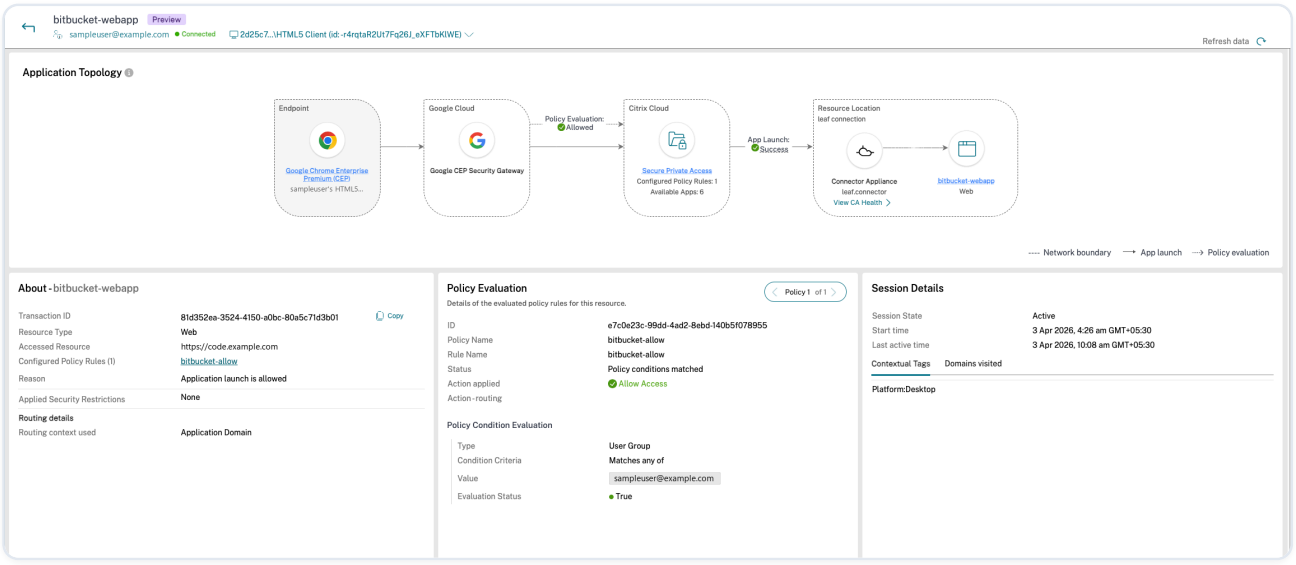
Visualizar uma sessão iniciada usando o Chrome Enterprise Premium na página Filtros

Você pode pesquisar as sessões do Chrome Enterprise Premium na página **Filtros**, onde o filtro Tipo de Cliente está disponível para localizar sessões específicas iniciadas usando o Chrome Enterprise Premium.



A página Gerenciador de Atividades fornece uma visão completa das transações de inicialização de aplicativos, resultados de políticas de acesso e erros de inicialização, juntamente com dados

de domínios visitados e eventos do ciclo de vida da sessão.



Observabilidade para VDA multi-sessão

O recurso de observabilidade para VDA multi-sessão aprimora os recursos de monitoramento e solução de problemas para sessões de Acesso Privado Seguro em um ambiente VDA multiusuário. Esse recurso capacita os Administradores de Suporte Técnico da Citrix a monitorar sessões de Acesso Privado Seguro, solucionar problemas e obter insights sobre inicializações de aplicativos e transações de usuários no caso de um VDA multi-sessão.

Principais recursos:

- Observabilidade aprimorada: Os administradores podem monitorar sessões do Secure Private Access, incluindo inicializações de aplicativos e enumerações, na interface do Citrix Director. Isso inclui visualizações detalhadas de problemas de enumeração e inicialização de aplicativos.
- Rastreamento de contexto do usuário: O recurso mantém o contexto do usuário para aplicativos acessados em um ambiente VDA compartilhado, garantindo visibilidade precisa dos dados da sessão para cada usuário.
- Insights de erro: Captura e exibe falhas de Single Sign-On (SSO), códigos de erro (por exemplo, 6003, 6007) e etapas de solução de problemas para resolver problemas.
- Pesquisa de sessão: Os administradores podem pesquisar sessões, aplicativos e transações de usuário usando o mesmo fluxo de trabalho que para sessões e aplicativos VDI.
- Navegação entre sessões: Permite a navegação entre sessões do Secure Private Access e sessões VDA para solução de problemas simplificada.

Cenários suportados:

- Ambiente VDA multiusuário: Suporta múltiplas sessões de usuário simultâneas acessando aplicativos internos, aplicativos SaaS e aplicativos web através do cliente Citrix Secure Access.
- Desktop de sessão única: Estende a mesma funcionalidade para desktops de sessão única para observabilidade consistente em todos os ambientes.

Tratamento de erros:

- Código de Erro 6003: Erro ao recuperar o manipular de logon único do Secure Private Access do serviço Broker Agent.
- Código de Erro 6007: Falha ao fazer login no Secure Private Access.
- Orientação para solução de problemas: Fornece descrições detalhadas de erros e links para etapas de solução de problemas dentro do Citrix Monitor.

Para obter mais informações, consulte O cliente Citrix Secure Access falhou ao fazer SSO na documentação do Citrix Secure Private Access.

Requisitos:

- Versão do Citrix Secure Access: Requer a versão 25.2.1.18 ou posterior do Citrix Secure Access para Windows.
- Serviço DaaS: O serviço DaaS deve estar acessível para solucionar problemas de sessões do Secure Private Access usando o Citrix Monitor.
- Implantação CAS: A implantação CAS deve estar disponível na região do Citrix Cloud onde o cliente está integrado.
- O agente Citrix Secure Access é auto-instalado e provisionado no VDI.
- As sessões do Secure Private Access são iniciadas para aplicativos web internos, aplicativos TCP/UDP e aplicativos SaaS roteados através de dispositivos de conector internos.

O recurso de Observabilidade para VDA multi-sessão fornece aos administradores ferramentas poderosas para monitorar, solucionar problemas e gerenciar sessões do Secure Private Access em um ambiente VDA multiusuário. Ao oferecer insights detalhados e fluxos de trabalho simplificados, este recurso aprimora a experiência geral de gerenciamento e garante a utilização eficiente dos recursos.

Solucionar problemas de acessibilidade de aplicativos (Connector Appliance para aplicativo de backend)

Quando um aplicativo Web, SaaS ou TCP/UDP entregue por meio do Secure Private Access™ falha ao iniciar, a causa é frequentemente um problema de rede entre o Connector Appliance e o servidor de aplicativos de backend. Até agora, os administradores não tinham uma maneira fácil de confirmar se o Connector Appliance poderia realmente alcançar o backend, ou de ver exatamente onde a conexão foi interrompida.

A opção **Executar sonda** no Monitor resolve isso. Ela permite que você acione uma sonda de rede sob demanda (um teste de conectividade) *de um Connector Appliance específico* para um host ou aplicativo de backend.

A sonda percorre cada estágio da conexão — resolução de DNS, conexão TCP, handshake TLS e a solicitação HTTP — e relata o resultado e o tempo gasto em cada estágio.

Isso ajuda você a confirmar rapidamente a acessibilidade e a identificar a etapa exata que falha, sem precisar fazer logon no console do Connector Appliance.

Você pode iniciar uma sonda de dois lugares no Monitor:

- A exibição de **Infraestrutura**, onde você escolhe qualquer Connector Appliance monitorado e sonda um host ou aplicativo arbitrário.
- A exibição de **Topologia de Aplicativos** de uma sessão do Secure Private Access, onde a sonda é oferecida em contexto quando o lançamento de um aplicativo falhou ao se conectar ao seu destino.

Requisitos

- Executar uma sonda é uma ação administrativa de solução de problemas. Você deve fazer login no Monitor como um administrador com permissões de administrador completas. A opção **Executar sonda** não está disponível para administradores de help desk.
- Você deve ter o direito de Secure Private Access para acionar uma sonda.
- O Connector Appliance deve ser monitorado na exibição de **Infraestrutura**. Para obter mais informações, consulte Monitoramento de infraestrutura.
- Para iniciar uma sonda a partir da exibição de topologia, você precisa de direitos de Citrix DaaS™ e Secure Private Access. Para obter mais informações, consulte Monitorar e solucionar problemas do Secure Private Access.

Protocolos e entradas da sonda

Ao iniciar uma sonda, você escolhe o **Protocolo** que corresponde ao backend que deseja testar. O protocolo determina quais estágios de conexão são testados e quais detalhes de destino você fornece.

PROTOCOLO	O QUE ELE TESTA	DETALHES DO DESTINO A SEREM FORNECIDOS
ICMP	Se o host de back-end responde a um ping do Connector Appliance.	Host de destino (endereço IP ou nome do host). Nenhuma porta é necessária.
TCP	Resolução de DNS e se uma conexão TCP pode ser aberta na porta.	Host e porta de destino.
SSL/TLS	Resolução de DNS, conexão TCP e o handshake TLS (incluindo negociação de certificado).	Host e porta de destino.
HTTP	Resolução de DNS, conexão TCP e a solicitação ou resposta HTTP.	URL do aplicativo.
HTTPS	Resolução de DNS, conexão TCP, handshake TLS e a solicitação ou resposta HTTPS.	URL do aplicativo.

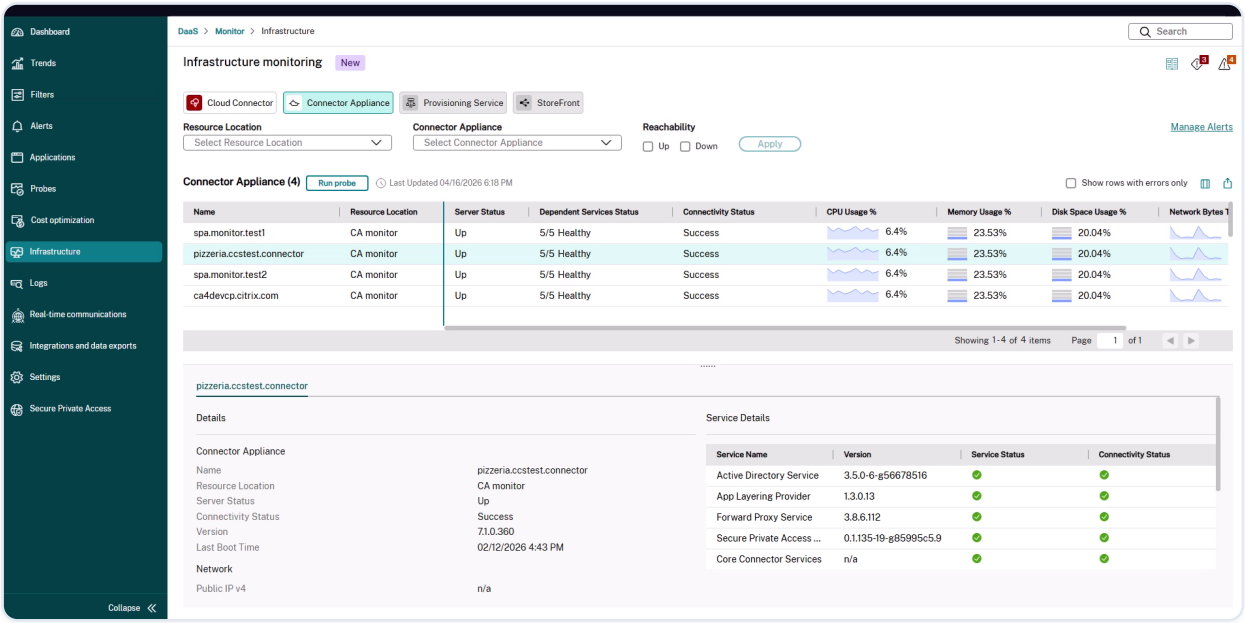
Você também pode escolher se a sonda é executada diretamente ou através de um proxy usando a lista **Proxy**:

- **Direto (sem proxy)** – O Connector Appliance se conecta diretamente ao destino.
- **\<proxy\>** – O Connector Appliance roteia a sonda através do proxy selecionado. A lista mostra os proxies (como `FQDN:PORT` ou `IP:PORT`) que estão disponíveis para a sonda.

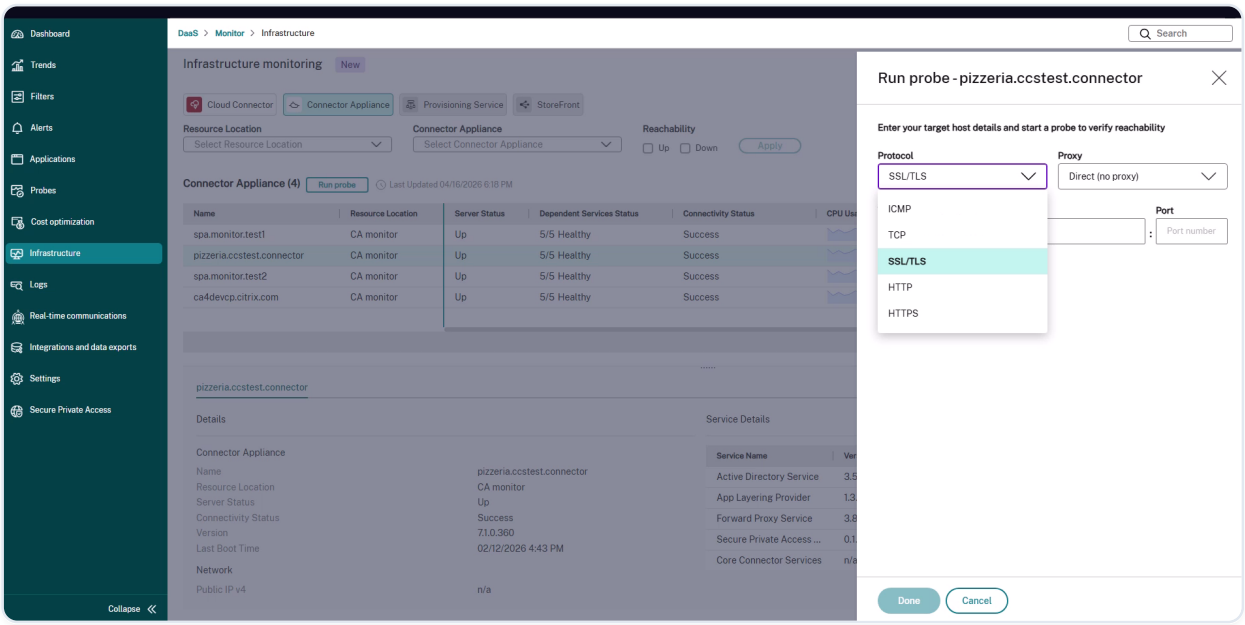
Executar uma sonda na visualização de Infraestrutura

Use este método quando quiser testar a acessibilidade a qualquer host ou aplicativo de um Connector Appliance escolhido — por exemplo, para verificar um servidor de back-end do qual um aplicativo depende.

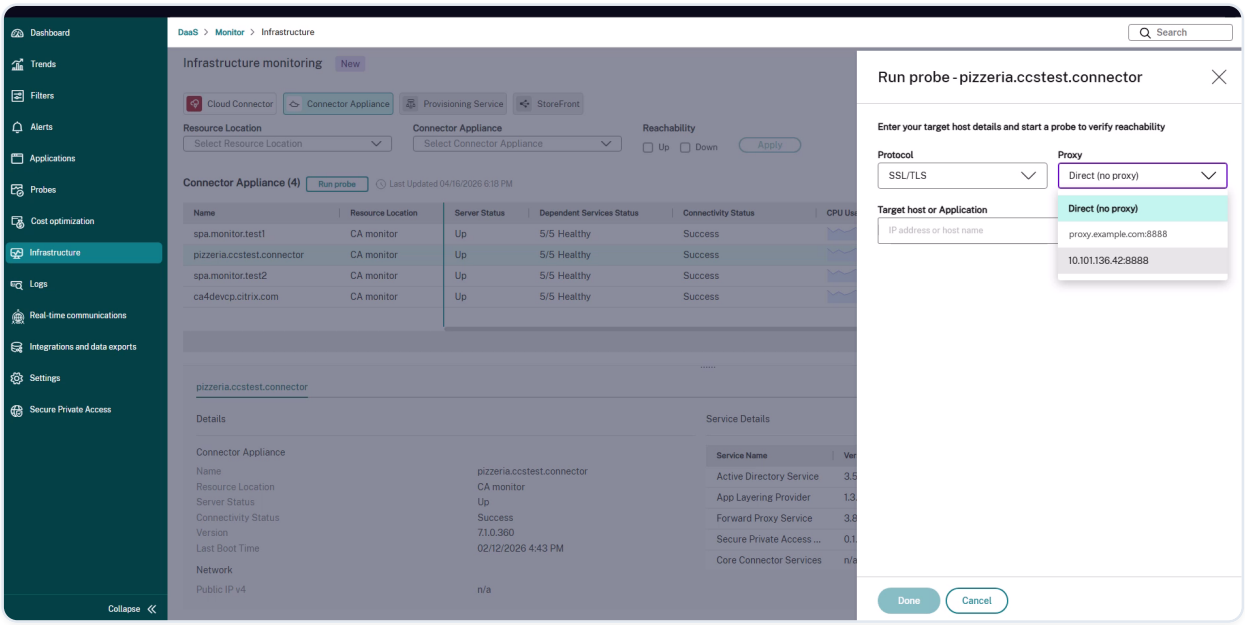
1. No Monitor, vá para **Infraestrutura** e selecione a guia **Connector Appliance**. A tabela lista os Connector Appliances monitorados com seu status de servidor, status de serviços dependentes, status de conectividade e uso de recursos.
2. Selecione a linha do Connector Appliance do qual você deseja sondar e clique em **Executar sonda**.



3. No painel **Executar sonda**, selecione um **Protocolo** e, se necessário, um **Proxy**.

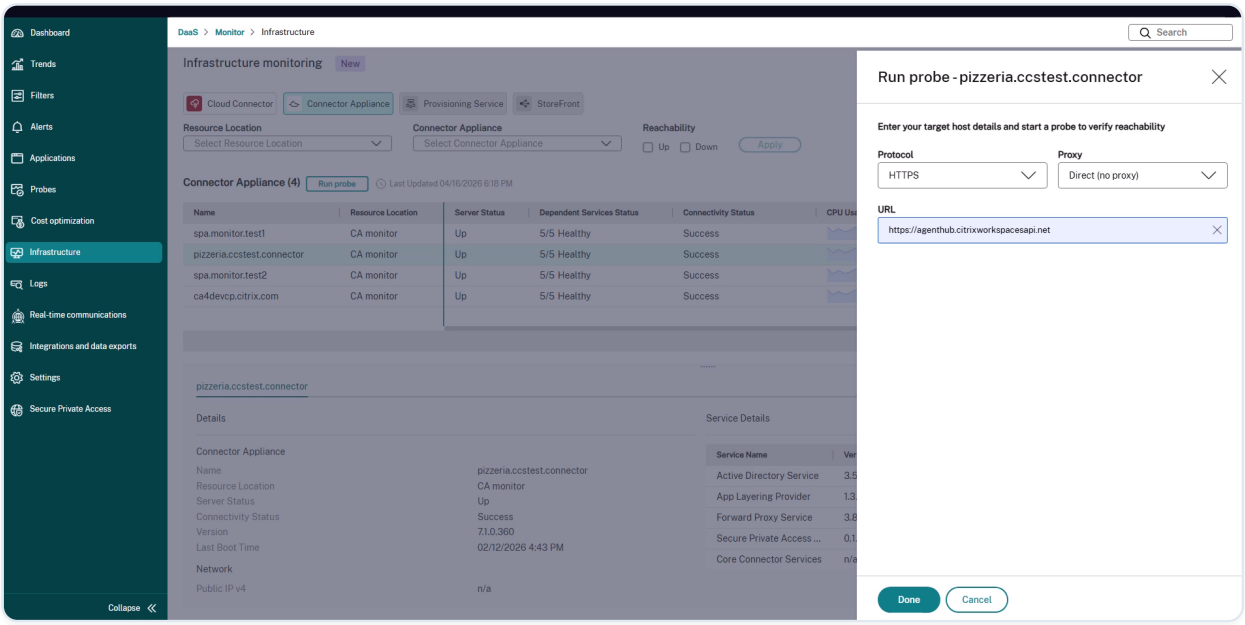


4. Se você quiser que a sonda passe por um proxy, selecione-o na lista **Proxy**. Caso contrário, deixe **Direto (sem proxy)** selecionado.



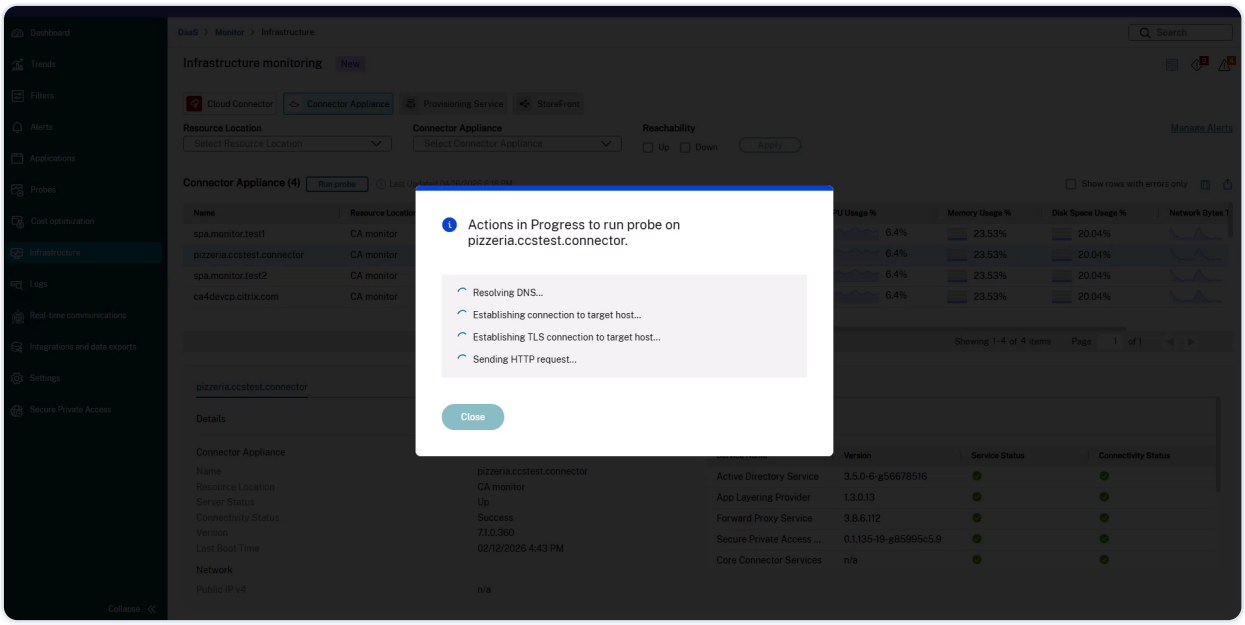
5. Insira os detalhes do destino para o protocolo selecionado:

   - Para **ICMP**, **TCP** e **SSL/TLS**, digite o **Host de destino ou Aplicativo** (endereço IP ou nome do host) e, quando aplicável, a **Porta**.
   - Para **HTTP** e **HTTPS**, digite a **URL** do aplicativo.



6. Clique em **Concluído** para iniciar a sonda.

   O Monitor exibe a caixa de diálogo **Ações em Andamento** e atualiza cada estágio da conexão à medida que é executado.



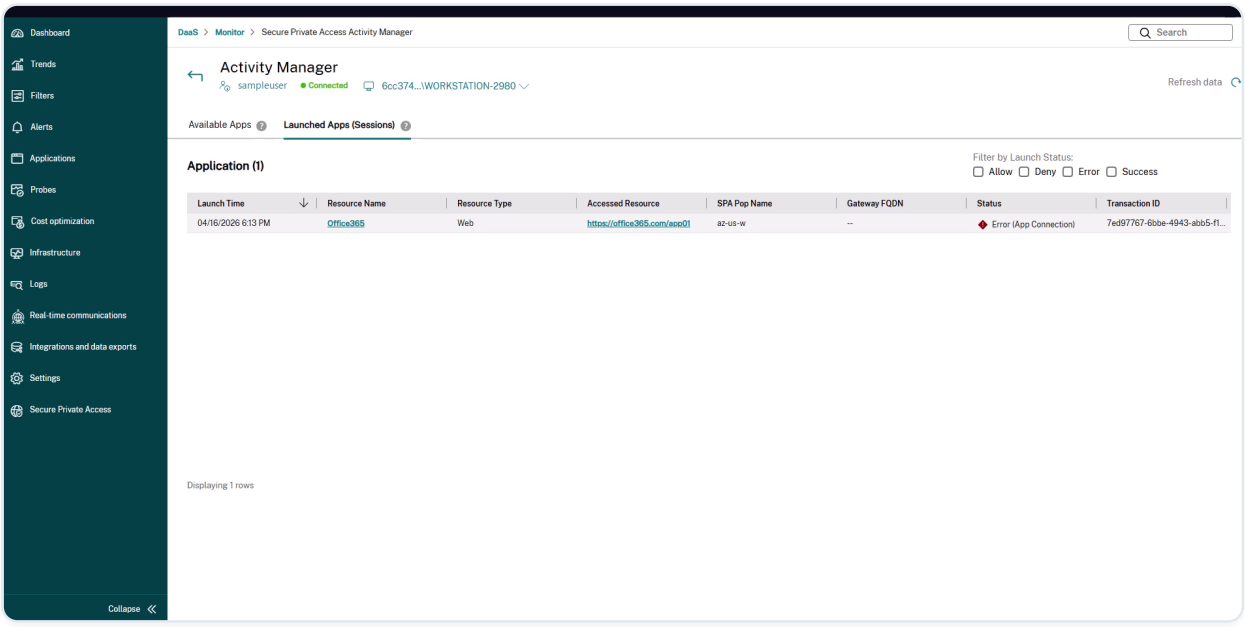
7. Quando a sonda terminar, revise o resultado. Para obter mais informações, consulte Entender os resultados da sonda. Clique em **Fechar** para fechar a caixa de diálogo.

Executar uma sonda a partir da visualização de Topologia de Aplicativos

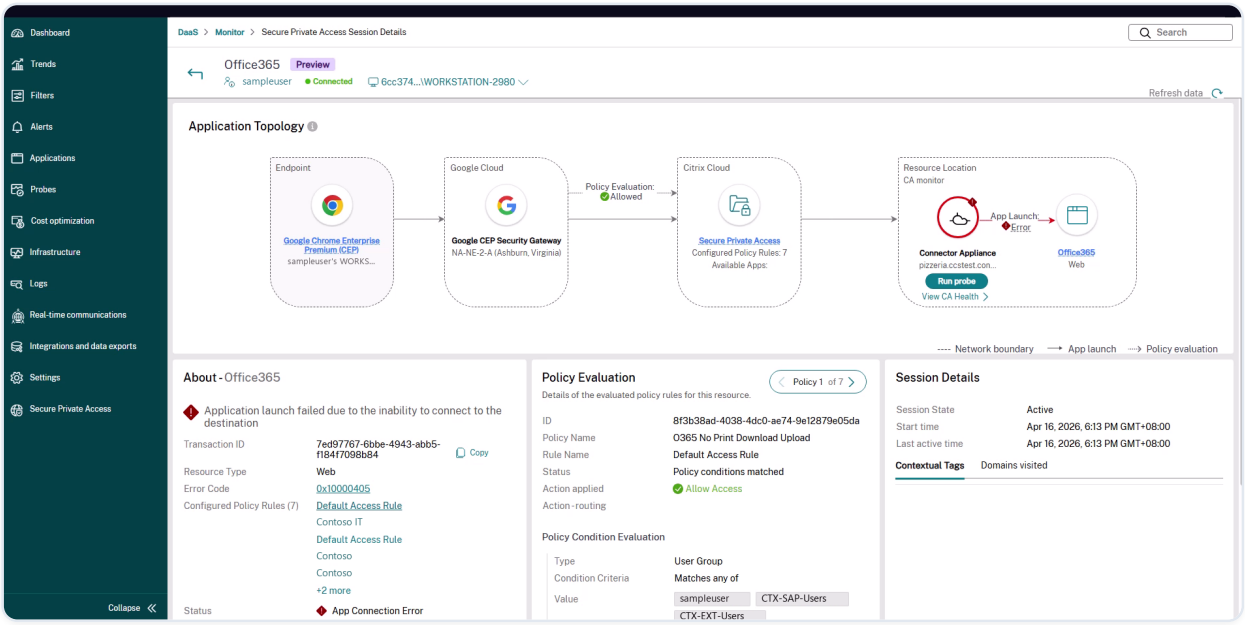
Use este método quando já estiver solucionando problemas de uma falha no lançamento de um aplicativo Secure Private Access. A sonda é oferecida em contexto, com o protocolo e o destino preenchidos a partir do aplicativo com falha.

Quando um aplicativo Web, SaaS ou TCP/UDP falha ao iniciar porque o Connector Appliance não consegue alcançar o backend, a **Topologia de Aplicativos** destaca o segmento entre o Connector Appliance e o aplicativo de backend como um **Erro de Lançamento de Aplicativo**, e o painel **Sobre** mostra *O lançamento do aplicativo falhou devido à incapacidade de conectar-se ao destino*.

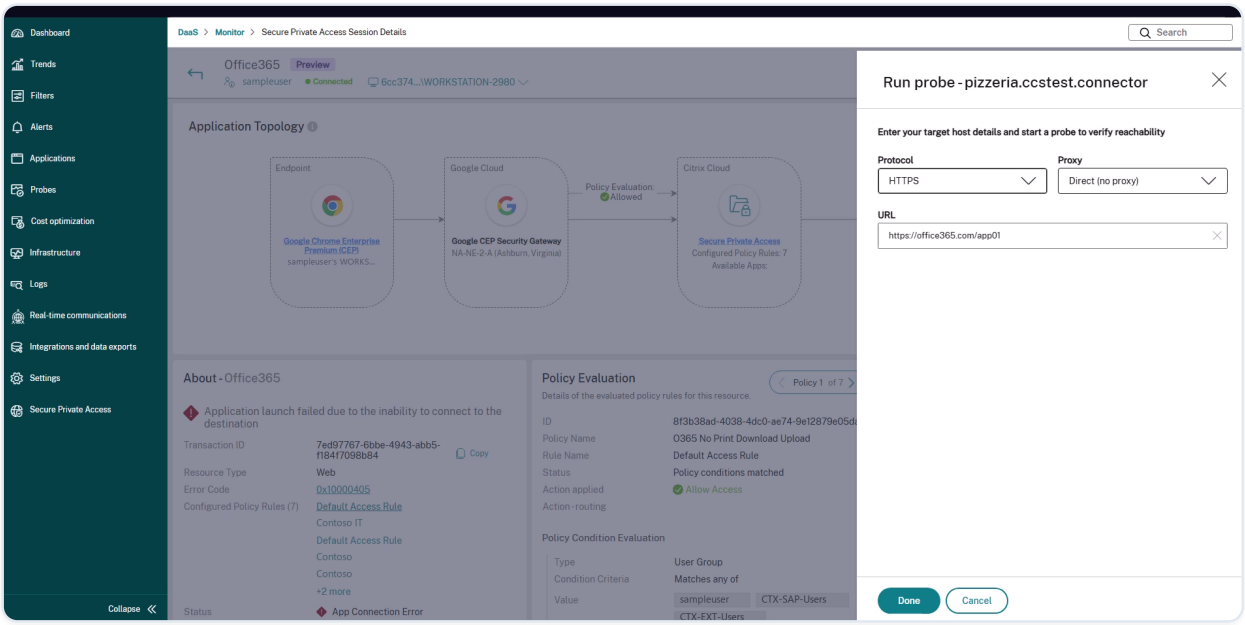
1. Abra a página **Detalhes da Sessão do Secure Private Access** para a sessão afetada. Um caminho típico é pesquisar o usuário, abrir o **Gerenciador de Atividades**, selecionar a guia **Aplicativos Lançados (Sessões)** e, em seguida, clicar no aplicativo que relata um status de **Erro (Conexão do Aplicativo)**. Para obter mais informações sobre como navegar para uma sessão, consulte Monitorar e solucionar problemas do Secure Private Access.



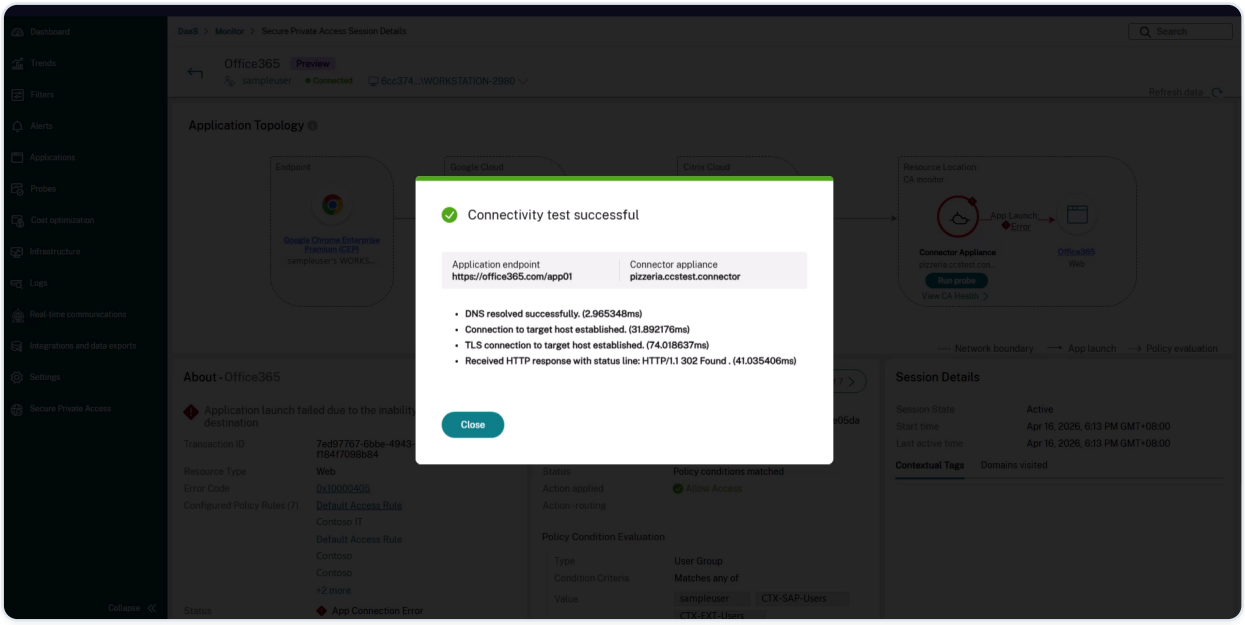
2. Na **Topologia de Aplicativos**, localize o nó **Connector Appliance** no **Local do Recurso**. Quando o lançamento falhou neste salto, o nó mostra um botão **Executar sonda** (e um link **Visualizar Integridade do CA**).



3. Clique em **Executar sonda**. O painel **Executar sonda** é aberto com o **Protocolo** e a **URL** do aplicativo preenchidos a partir do lançamento com falha. Ajuste os detalhes, se necessário.



4. Clique em **Concluído** para iniciar a sonda, e em seguida, revise o resultado quando ela terminar.



A execução da sonda confirma se o Connector Appliance selecionado pode alcançar o endpoint do aplicativo. Se a sonda for bem-sucedida enquanto o aplicativo ainda falha ao iniciar, você pode descartar a capacidade de alcance do Connector Appliance para o backend e focar sua investigação em outro lugar. Se a sonda falhar, o resultado mostra o estágio que falhou, o que o direciona para o problema subjacente de rede ou backend.

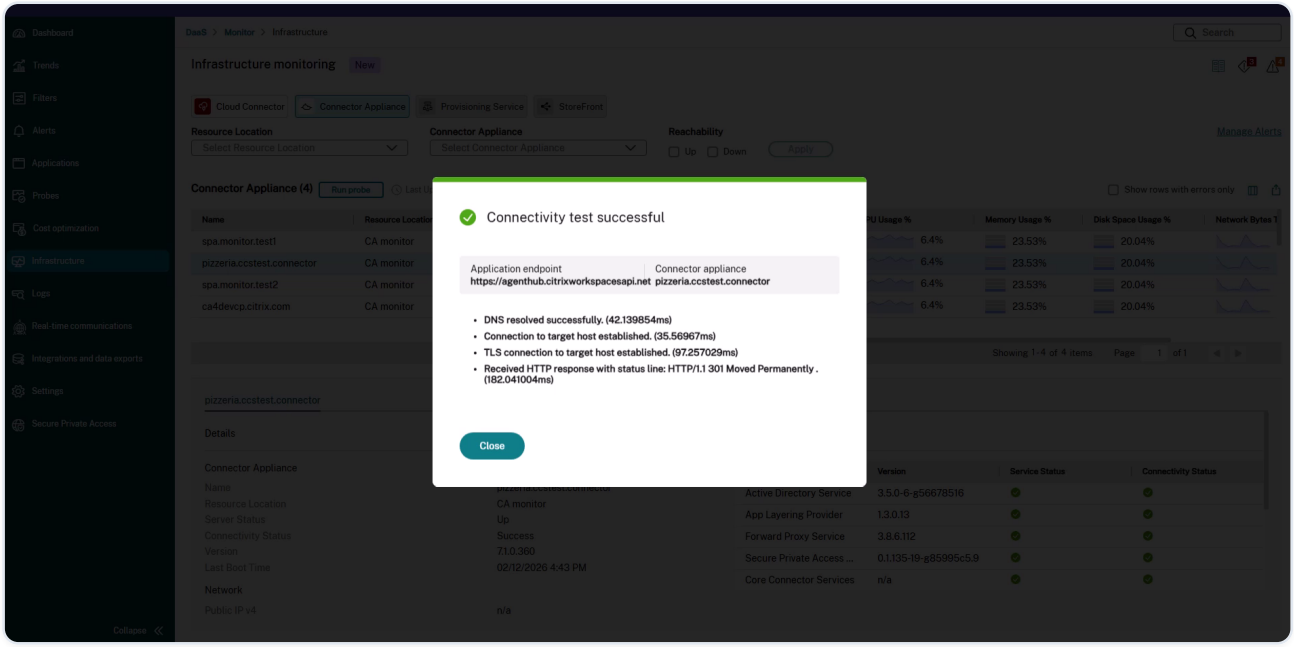
Entender os resultados da sonda

Após a conclusão da sonda, o Monitor mostra o resultado para cada estágio de conexão, juntamente com o tempo gasto. A caixa de diálogo também mostra o **endpoint do aplicativo** que foi testado e o **Connector Appliance** que executou a sonda.

Sonda bem-sucedida

Se todas as etapas forem bem-sucedidas, a caixa de diálogo mostra **Teste de conectividade bem-sucedido** e lista cada etapa concluída — por exemplo:

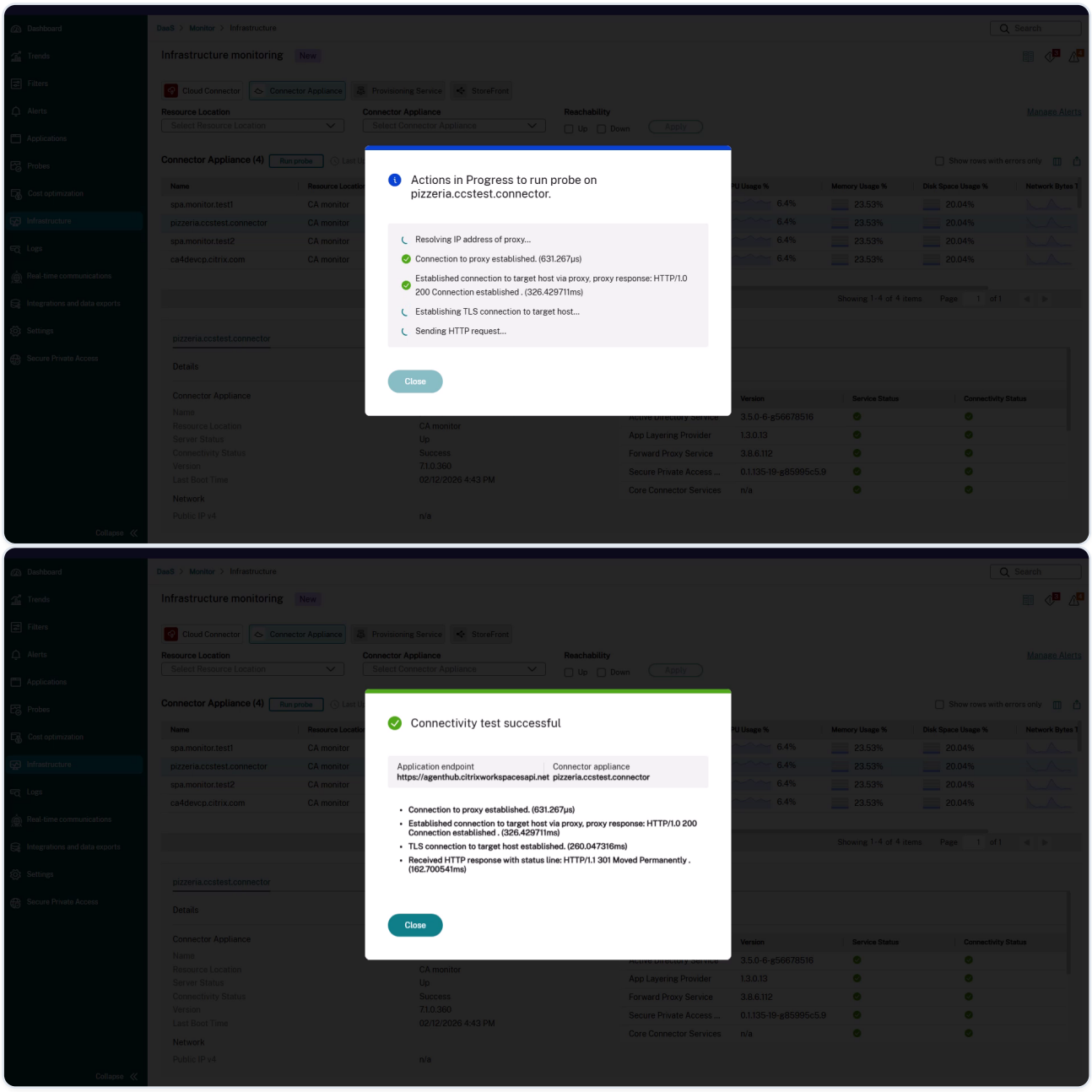
- DNS resolvido com sucesso.
- Conexão com o host de destino estabelecida.
- Conexão TLS com o host de destino estabelecida.
- Resposta HTTP recebida com linha de status: `HTTP/1.1 301 Moved Permanently`.



> **Nota:**
>
> Os estágios mostrados dependem do protocolo. Por exemplo, o estágio TLS aparece apenas para sondas **SSL/TLS** e **HTTPS**, e o estágio de solicitação ou resposta HTTP aparece apenas para sondas **HTTP** e **HTTPS**.

Sondar através de um proxy

Quando você executa a sonda através de um proxy, o resultado inclui os estágios de conexão do proxy antes dos estágios do host de destino — por exemplo, *Conexão com o proxy estabelecida* e *Conexão estabelecida com o host de destino via proxy*.



Sonda com falha

Se um estágio falhar, o resultado identifica o estágio que falhou e mostra os detalhes do erro associado (por exemplo, um erro de conexão TCP como *Conexão recusada*). Como a sonda é executada a partir do Connector Appliance selecionado, o estágio com falha informa onde o caminho se rompe:

- **A resolução DNS falha** – O Connector Appliance não consegue resolver o nome do host. Verifique a configuração de DNS e o nome do host ou URL que você inseriu.
- **A conexão TCP falha** – O host está inacessível ou a porta está fechada ou bloqueada. Verifique o host de destino, a porta, as regras de firewall e se o serviço de back-end está em execução.

- **O handshake TLS falha** – A conexão TCP é bem-sucedida, mas a negociação TLS falha. Verifique o certificado, a versão TLS e o SNI ou nome do host.
- **A solicitação HTTP falha** – A conexão é bem-sucedida, mas o aplicativo retorna um erro ou não responde. Verifique o aplicativo e o caminho do URL.

Considerações

- Uma sonda é um teste de conectividade sob demanda e pontual. Ela não fornece monitoramento contínuo.
- A sonda é executada a partir do caminho de dados do Connector Appliance selecionado, portanto, o resultado reflete a visão de rede desse Connector Appliance.
- Espera-se que uma sonda seja concluída em cerca de dois minutos.
- A coleta de um rastreamento de pacotes do Connector Appliance não é suportada pelo Monitor. Se um rastreamento de pacotes for necessário, o administrador de rede deve coletá-lo no console do Connector Appliance.
- O valor de **Latência da Conexão** no salto do Connector Appliance para o aplicativo de back-end na Topologia do Aplicativo é uma medição passiva e periódica (P90 na última hora). Use uma sonda quando precisar de um teste de acessibilidade sob demanda e pontual para esse salto. Para obter mais informações, consulte Latência do Connector Appliance para o aplicativo de back-end.

Granularidade e retenção de dados

Agregação de valores de dados

O Serviço Monitor coleta vários dados, incluindo uso da sessão do usuário, detalhes de desempenho de logon do usuário, detalhes de balanceamento de carga da sessão e informações de falha de conexão e máquina. Os dados são agregados de forma diferente dependendo de sua categoria. Compreender a agregação dos valores de dados apresentados usando as APIs do Método OData é fundamental para interpretar os dados. Por exemplo:

- Sessões Conectadas e Falhas de Máquina ocorrem durante um período. Portanto, são expostas como máximos durante um período de tempo.
- A Duração do Logon é uma medida do período de tempo, portanto, é exposta como uma média durante um período de tempo.
- A Contagem de Logons e as Falhas de Conexão são contagens de ocorrências durante um período, portanto, são expostas como somas durante um período de tempo.

Avaliação de dados concorrentes

Suas sessões devem ser sobrepostas para serem consideradas concorrentes. No entanto, quando o intervalo de tempo é de 1 minuto, todas as sessões nesse minuto (independentemente de se sobreporem) são consideradas concorrentes. O tamanho do intervalo é tão pequeno que a sobrecarga de desempenho envolvida no cálculo da precisão não compensa o valor adicionado. Se as sessões ocorrerem na mesma hora, mas não no mesmo minuto, elas não são consideradas sobrepostas.

Correlação de tabelas de resumo com dados brutos

O modelo de dados representa métricas de duas maneiras diferentes:

- As tabelas de resumo representam visualizações agregadas das métricas em granularidades de tempo por minuto, hora e dia.
- Os dados brutos representam eventos individuais ou o estado atual rastreado na sessão, conexão, aplicativo e outros objetos.

Ao tentar correlacionar dados entre chamadas de API ou dentro do próprio modelo de dados, é importante entender os seguintes conceitos e limitações:

- **Nenhum dado de resumo para intervalos parciais.** Os resumos de métricas são projetados para atender às necessidades de tendências históricas em longos períodos. Essas métricas são agregadas na tabela de resumo para intervalos completos. Não há dados de resumo para um intervalo parcial no início (dados mais antigos disponíveis) da coleta de dados nem no final. Ao visualizar agregações de um dia (Interval=1440), isso significa que os primeiros e os mais recentes dias incompletos não têm dados. Embora dados brutos possam existir para esses intervalos parciais, eles nunca são resumidos. Puxe o min e o max SummaryDate de uma tabela de resumo específica para determinar o intervalo agregado mais antigo e mais recente para uma granularidade de dados específica. A coluna SummaryDate representa o início do intervalo. A coluna Granularity representa a duração do intervalo para os dados agregados.
- **Correlação por tempo.** As métricas são agregadas na tabela de resumo para intervalos completos, conforme descrito na seção anterior. Elas podem ser usadas para tendências históricas, mas os eventos brutos podem estar mais atualizados no estado do que o que foi resumido para análise de tendências. Qualquer comparação baseada em tempo de dados de resumo com dados brutos deve levar em consideração que não há dados de resumo para intervalos parciais que possam ocorrer ou para o início e o fim do período de tempo.

- **Eventos perdidos e latentes.** As métricas agregadas na tabela de resumo podem ser ligeiramente imprecisas se os eventos forem perdidos ou latentes para o período de agregação. Embora o Serviço de Monitoramento tente manter um estado atual preciso, ele não volta no tempo para recalcular a agregação nas tabelas de resumo para eventos perdidos ou latentes.
- **Alta disponibilidade de conexão.** Durante a HA de conexão, há lacunas nas contagens de dados de resumo das conexões atuais, mas as instâncias de sessão ainda estão sendo executadas nos dados brutos.
- **Períodos de retenção de dados.** Os dados nas tabelas de resumo são retidos em um cronograma de limpeza diferente do cronograma para dados de eventos brutos. Os dados podem estar ausentes porque foram limpos das tabelas de resumo ou brutas. Os períodos de retenção também podem diferir para diferentes granularidades de dados de resumo. Dados de granularidade inferior (minutos) são limpos mais rapidamente do que dados de granularidade superior (dias). Se os dados estiverem ausentes de uma granularidade devido à limpeza, eles poderão ser encontrados em uma granularidade superior. Como as chamadas de API retornam apenas a granularidade específica solicitada, não receber dados para uma granularidade não significa que os dados não existam para uma granularidade superior para o mesmo período de tempo.
- **Fusos horários.** As métricas são armazenadas com carimbos de data/hora UTC. As tabelas de resumo são agregadas em limites de fuso horário por hora. Para fusos horários que não se enquadram nos limites por hora, pode haver alguma discrepância quanto ao local onde os dados são agregados.

Granularidade e retenção

A granularidade dos dados agregados recuperados pelo Monitor é uma função do período de tempo (T) solicitado. As regras são as seguintes:

- 0 \< T \<= 30 dias usam granularidade por hora
- T \> 31 dias usam granularidade por dia

Os dados solicitados que não vêm de dados agregados vêm das informações brutas de Sessão e Conexão. Esses dados tendem a crescer rapidamente e, portanto, têm sua própria configuração de limpeza. A limpeza garante que apenas dados relevantes sejam mantidos a longo prazo. Isso garante melhor desempenho, mantendo a granularidade necessária para relatórios.

#	NOME DA CONFIGURAÇÃO	TABELA DE ESQUEMA IMPACTADA	TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
1	GroomSessionsRetentionDays	Tabelas MonitorData.Session e Monitordata.Connection	Essa configuração afeta os detalhes da sessão, Duração do Logon por Sessão do Usuário, tabelas de Uso Baseado em Aplicativo na página Tendências.	90	31
2	GroomFailuresRetentionDays	MonitorData.MachineFailureLog e MonitorData.ConnectionFailureLog	Página Tendências: Essa configuração afeta gráficos e tabelas na guia de falhas.	90	31
3	GroomLoadIndexesRetentionDays	MonitorData.LoadIndex	Essa configuração afeta os dados exibidos na guia "Load Evaluator Index" na	3	3

#	NOME DA CONFIGURAÇÃO	TABELA DE ESQUEMA IMPACTADA	TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
			página Tendências.		
4	GroomDeletedRetentionDays	Entidades MonitorData.Machine, MonitorData.Catalog, MonitorData.DesktopGroup e MonitorData.Hypervisor que têm um LifecycleState de 'Deleted'. Essa configuração também exclui quaisquer registros relacionados de Session, SessionDetail, Summary, Failure ou LoadIndex.	Entidades Machine, Catalog, DesktopGroup e Hypervisor que têm um LifecycleState de 'Deleted'. Essa configuração também exclui quaisquer registros relacionados de Session, SessionDetail, Summary, Failure ou LoadIndex.	90	31
5	GroomSummariesRetentionDays	MonitorData.DesktopGroupSummary, MonitorData	Essa configuração afeta todos os	365	31

#	NOME DA CONFIGURAÇÃO	TABELA DE ESQUEMA IMPACTADA	TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
		.FailureLogSummary e MonitorData.LoadIndexSummary	dados do gráfico na página Tendências.		
6	GroomMachineHotfixLogRetentionDays	MonitorData.Hotfix	Esta configuração afeta os dados de hotfix do VDA mostrados na página Detalhes da Máquina.	90	31
7	GroomHourlyRetentionDays	todas as tabelas de Resumo	Isso afeta os gráficos semanais mostrados na página Tendências.	32	31
8	GroomApplicationInstanceRetentionDays	MonitorData.ApplicationInstance	Essa configuração afeta o gráfico e as tabelas na guia Gerenciamento de capacidade e as tabelas de uso de aplicativos	90	Não aplicável

#	NOME DA CONFIGURAÇÃO	TABELA DE ESQUEMA IMPACTADA	TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
			na página Tendências.		
9	GroomNotificationLogRetentionDays	MonitorData.NotificationLog	Essa configuração afeta os Alertas exibidos no Monitor.	90	Não aplicável
10	GroomResourceUsageRawDataRetentionDays	MonitorData.Resourceutilization	Essa configuração afeta os gráficos de CPU e Memória vistos na página Detalhes da Máquina, em "Utilização Histórica da Máquina", e o cálculo de dados na área de Otimização de custos, na guia "Dimensionamento de carga de trabalho".	3	3

#	NOME DA CONFIGURAÇÃO	TABELA DE ESQUEMA IMPACTADA	TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
11	GroomResourceUsageHourDataRetentionDays	MonitorData.Resourceutilizationsummary	Essa configuração afeta os gráficos de CPU e Memória vistos na página de Detalhes da Máquina "Utilização Histórica da Máquina" e o cálculo de dados na área de otimização de custos "Guia de dimensionamento de carga de trabalho".	30	30
12	GroomResourceUsageDayDataRetentionDays	MonitorData.Resourceutilizationsummary	Essa configuração afeta o gráfico de CPU e Memória visto em "Utilização de recursos" da Máquina na página	365	31

#	NOME DA CONFIGURAÇÃO	TABELA DE ESQUEMA IMPACTADA	TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
			Tendências e na página "Utilização da máquina" para uma máquina específica.		
13	GroomProcessUsageRawDataRetentionDays	MonitorData.ProcessUtilization	Esta configuração afeta a tendência de recursos por informações de processo mostradas na página de uso histórico da máquina.	1	1
14	GroomProcessUsageHourDataRetentionDays	MonitorData.ProcessUtilizationHourSummary	Esta configuração afeta a tendência de uso de CPU e Memória por processo mostrada na página de uso histórico da máquina.	7	7

#	NOME DA CONFIGURAÇÃO	TABELA DE ESQUEMA IMPACTADA	TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
15	GroomProcessUsageDayDataRetentionDays	MonitorData.ProcessUtilizationDaySummary	Esta configuração afeta a tendência de uso de CPU e Memória por processo mostrada na página de uso histórico da máquina.	30	30
16	GroomSessionMetricsDataRetentionDays	MonitorData.Sessionmetrics	Esta configuração afeta todos os gráficos vistos na guia "Desempenho da Sessão" da página de detalhes do usuário.	1	1
17	GroomMachineMetricDataRetentionDays	MonitorData.Machinemetrics	Esta configuração afeta o gráfico e a tabela na guia "Utilização de	3	3

#	NOME DA CONFIGURAÇÃO	TABELA DE ESQUEMA IMPACTADA	TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
			Recursos" na página Tendências.		
18	GroomMachineMetricDaySummaryDataRetentionDays	MonitorData.MachineMetricDaySummary	Esta configuração o afeta o gráfico e a tabela na guia "Utilização de Recursos" na página Tendências.	365	31
19	GroomApplicationErrorsRetentionDays	MonitorData.ApplicationError	Esta configuração o afeta os detalhes de erro mostrados na coluna "Erros de Aplicativo" na página Aplicativos.	1	1
20	GroomApplicationFaultsRetentionDays	MonitorData.Applicationfailure	Esta configuração o afeta a coluna "Falhas de Aplicativo"	1	1

#	NOME DA CONFIGURAÇÃO	TABELA DE ESQUEMA IMPACTADA	TABELAS E GRÁFICO IMPACTADOS NAS PÁGINAS DO MONITOR	DIAS DE RETENÇÃO PARA PREMIUM	DIAS DE RETENÇÃO PARA ADVANCED
			na página Aplicativos.		

Cuidado:

Não é possível modificar os valores no banco de dados do Serviço de Monitoramento.

A retenção de dados por longos períodos tem as seguintes implicações no tamanho das tabelas:

- **Dados por hora.** Se os dados por hora puderem permanecer no banco de dados por até dois anos, um site de 1000 grupos de entrega pode fazer com que o banco de dados cresça da seguinte forma:

  1000 grupos de entrega x 24 horas/dia x 365 dias/ano x 2 anos = 17.520.000 linhas de dados. O impacto no desempenho de uma quantidade tão grande de dados nas tabelas de agregação é significativo. Dado que os dados do painel são extraídos desta tabela, os requisitos no servidor de banco de dados podem ser grandes. Quantidades excessivamente grandes de dados podem ter um impacto dramático no desempenho.
- **Dados de sessão e evento.** Estes são os dados coletados cada vez que uma sessão é iniciada e uma conexão/reconexão é feita. Para um site grande (100 mil usuários), esses dados crescem rapidamente. Por exemplo, o equivalente a dois anos dessas tabelas reuniria mais de um TB de dados, exigindo um banco de dados de nível empresarial de ponta.

Diagnóstico de inicialização de sessão

Nota:

O diagnóstico de inicialização de sessão está atualmente em pré-visualização.

> As inicializações de sessão envolvem vários componentes Citrix. Para diagnosticar falhas de inicialização de sessão, use o Citrix Monitor (ou seja, o serviço Citrix Director) para identificar o componente exato e o estágio onde o problema ocorreu. Aplique as ações recomendadas para resolver o problema. O aplicativo Citrix Workspace™ gera um ID de Transação de 32 dígitos (8-4-4-4-12) que pode ser usado no diagnóstico de falhas de inicialização de sessão.

> **Nota:**
>
> Este recurso está disponível apenas para clientes em nuvem nas regiões dos EUA, AP-S e UE. Não está disponível no Japão e nas regiões governamentais.

Pré-requisitos

Se você estiver usando o Citrix DaaS™, o onboarding é automático. Clientes em nuvem que usam o StoreFront local devem garantir que uma versão compatível do StoreFront esteja integrada.

- Se você estiver usando o Citrix Analytics for Performance, consulte Fontes de dados para obter as etapas para integrar o StoreFront local.
- Se você não estiver usando o Citrix Analytics for Performance™:

  a. Vá para `https://analytics.cloud.com/unified-datasources/perf/Citrix%20Virtual%20Apps%20and%20Desktops/site-details`.

  b. Clique em **Conectar à implantação do StoreFront**, insira os detalhes e baixe o arquivo de configuração. Para obter mais informações, consulte Integração de sites locais usando o StoreFront.

  > **Nota:**
  >
  > Administradores com funções de Administrador de Nuvem têm permissão para integrar implantações do StoreFront™, enquanto administradores com funções de Administrador de Monitor Completo só podem visualizar as implantações do StoreFront.

As versões mínimas suportadas de outros componentes são as seguintes:

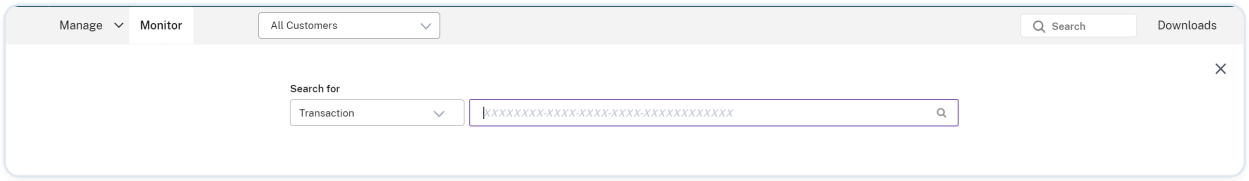
- Citrix Workspace app para Windows 2109

- Citrix Workspace app para Mac 2112
- Citrix Workspace app para Linux 2112
- Citrix Workspace app para HTML5 2110
- Citrix Workspace app para Chrome 2110
- Citrix Workspace app para Android 2110
- Versão VDA Citrix Virtual Apps and Desktops™ 2112
- Citrix StoreFront 1912 LTSR CU4

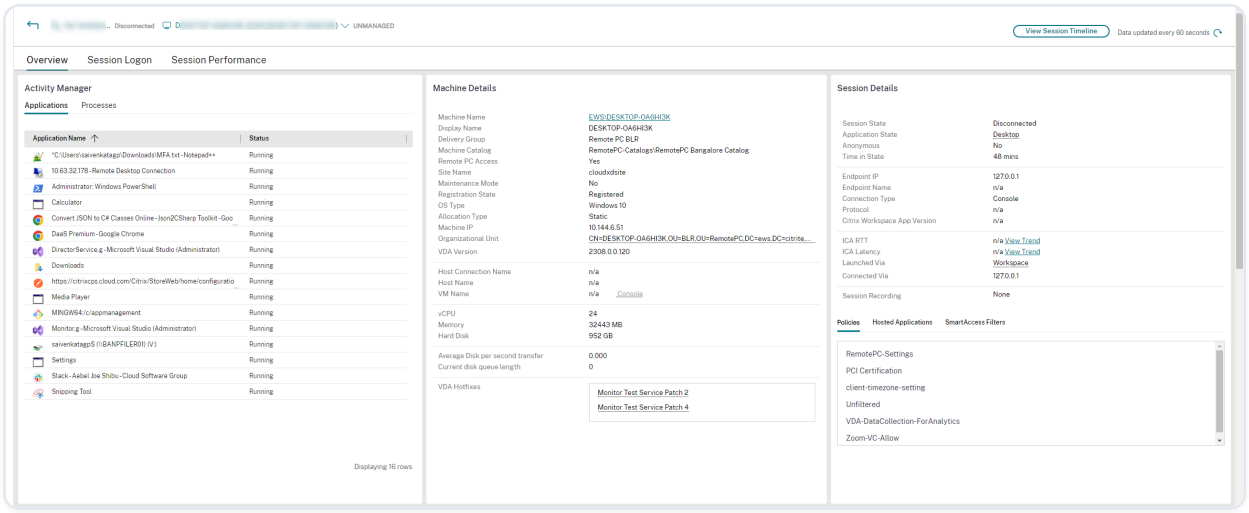
Etapas para diagnosticar falha no lançamento da sessão

1. Copie o ID da Transação do lançamento de sessão com falha do Citrix Workspace app.

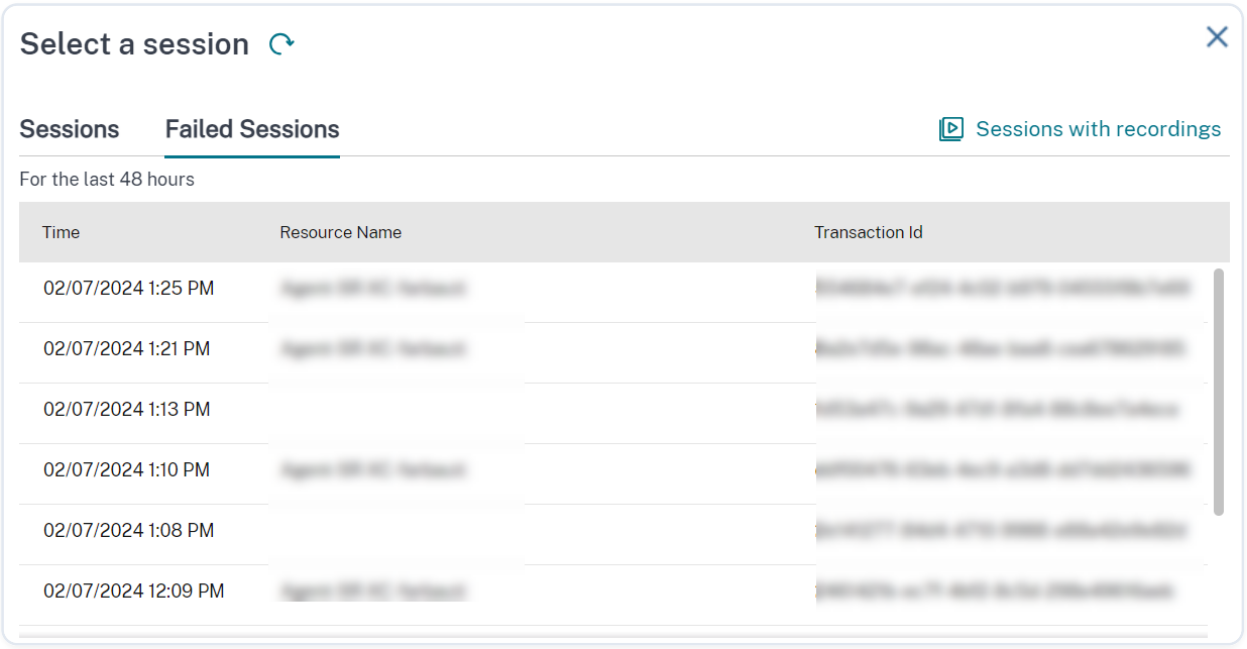
2. Na interface do usuário do Monitor, procure o ID da transação de 32 dígitos e clique em **Detalhes**.



3. Se o ID da Transação não estiver disponível, pesquise usando o nome de usuário. O Gerenciador de Atividades do usuário é exibido.



4. Clique no seletor de sessão. Vá para a guia **Sessões com Falha**. Uma lista de sessões que falharam nas últimas 48 horas é exibida. Clique na sessão selecionada.



5. O Citrix Monitor exibe componentes, detalhes de erro e detalhes do log de transações referentes à transação.

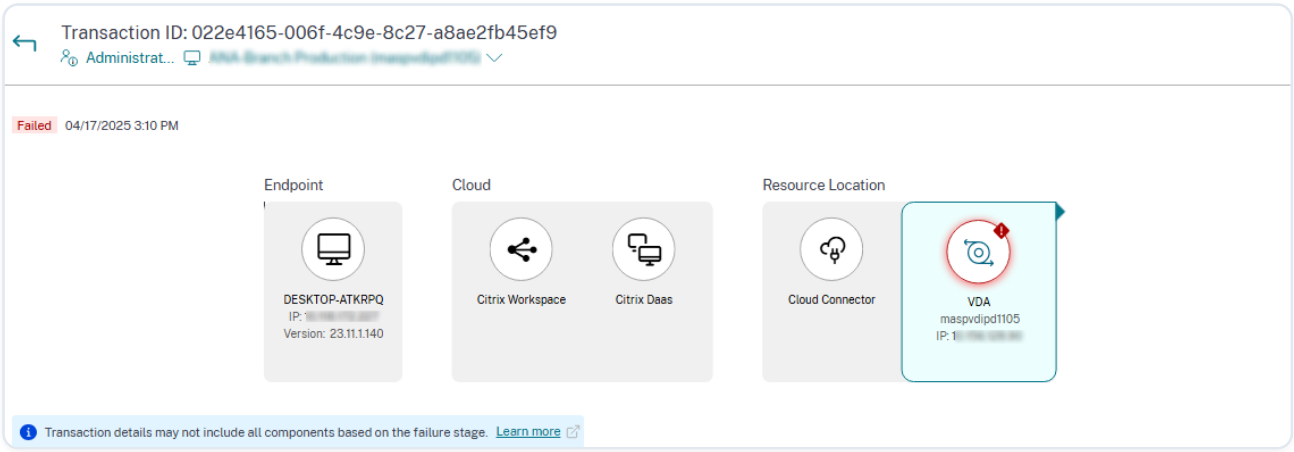
A tela anterior mostra as seguintes seções:

- Componentes
- Detalhes do Erro
- Logs de Transação

Componentes

Dependendo do cenário de inicialização da sessão e do estágio da falha, os componentes envolvidos em uma sessão são qualquer um dos seguintes:

- Ponto de extremidade
- Citrix® StoreFront Cloud
- Citrix DaaS
- Cloud Connector
- Gateway Service
- VDA
- Citrix StoreFront



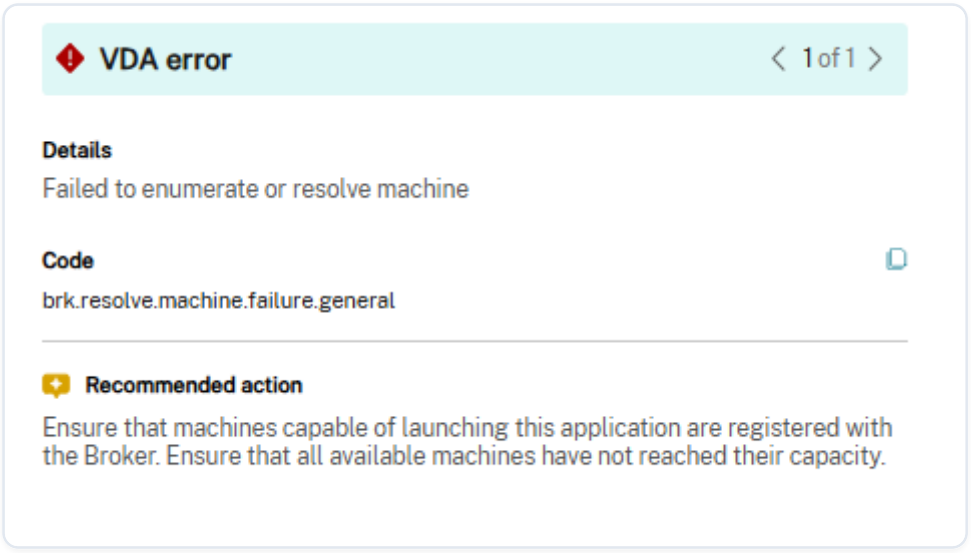
Os componentes onde a falha ocorre são destacados na imagem anterior.

Nota:

- Os componentes da transação são determinados pelos eventos de lançamento de sessão recebidos. Se uma falha ocorrer no início do processo, ou se os eventos não forem recebidos, alguns componentes podem não ser exibidos. Por exemplo, se o erro ocorreu na comunicação entre o aplicativo Citrix Workspace e o Citrix® StoreFront Cloud, os componentes seriam apenas Endpoint e Citrix® StoreFront Cloud.
- Em certos casos extremos, uma transação pode ser considerada falha, mas nenhum erro é relatado, desde que nenhum evento de falha seja recebido.
- Os códigos de erro do lado do cliente e as informações de diagnóstico estão disponíveis apenas quando o Citrix StoreFront está integrado e enviando dados. Para obter mais informações sobre a integração do StoreFront, consulte Pré-requisitos. Esta é uma das razões pelas quais nenhum erro é relatado para uma sessão com falha.

Detalhes do erro

Os detalhes do erro destacam qual problema ocorreu em um determinado componente. A descrição do erro, o código do erro e a ação recomendada são exibidos.

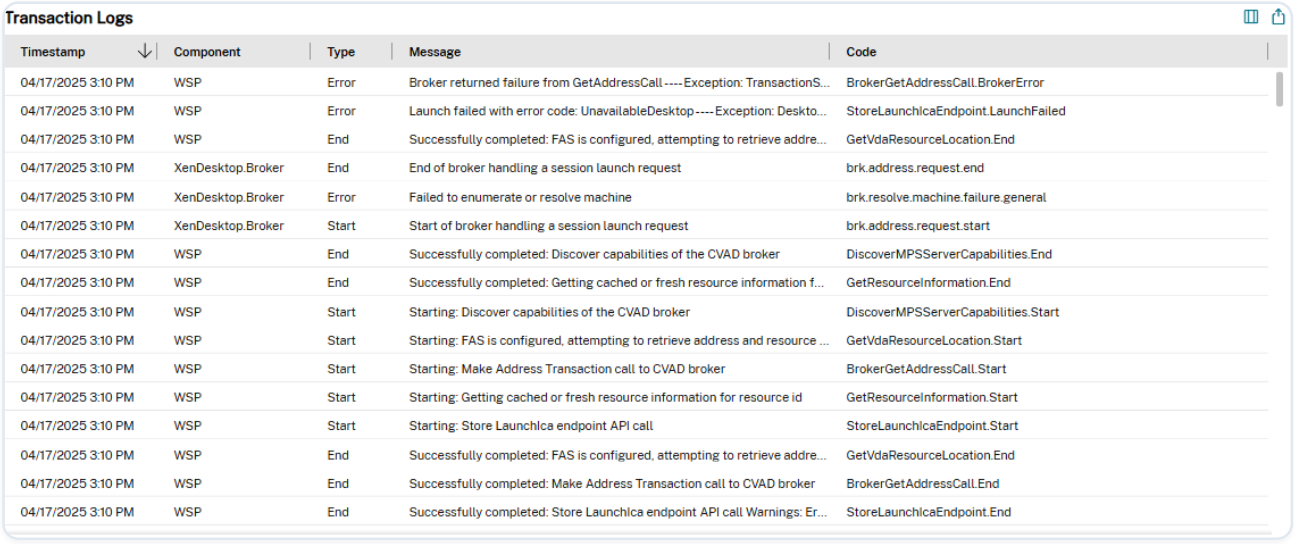


Nota:

Esta seção exibe apenas a causa raiz dos erros, não todos os erros individuais dos eventos brutos. Para logs individuais, consulte os logs de transação.

Logs de Transação

Os Logs de Transação fornecem os eventos brutos de lançamento de sessão, oferecendo um rastreamento de ponta a ponta entre os componentes envolvidos na conexão.



Transaction Logs

Timestamp	Component	Type	Message	Code
04/17/2025 3:10 PM	WSP	Error	Broker returned failure from GetAddressCall ----Exception: TransactionS...	BrokerGetAddressCall.BrokerError
04/17/2025 3:10 PM	WSP	Error	Launch failed with error code: UnavailableDesktop ----Exception: Deskto...	StoreLaunchIcaEndpoint.LaunchFailed
04/17/2025 3:10 PM	WSP	End	Successfully completed: FAS is configured, attempting to retrieve addre...	GetVdaResourceLocation.End
04/17/2025 3:10 PM	XenDesktop.Broker	End	End of broker handling a session launch request	brk.address.request.end
04/17/2025 3:10 PM	XenDesktop.Broker	Error	Failed to enumerate or resolve machine	brk.resolve.machine.failure.general
04/17/2025 3:10 PM	XenDesktop.Broker	Start	Start of broker handling a session launch request	brk.address.request.start
04/17/2025 3:10 PM	WSP	End	Successfully completed: Discover capabilities of the CVAD broker	DiscoverMPSServerCapabilities.End
04/17/2025 3:10 PM	WSP	End	Successfully completed: Getting cached or fresh resource information f...	GetResourceInformation.End
04/17/2025 3:10 PM	WSP	Start	Starting: Discover capabilities of the CVAD broker	DiscoverMPSServerCapabilities.Start
04/17/2025 3:10 PM	WSP	Start	Starting: FAS is configured, attempting to retrieve address and resource ...	GetVdaResourceLocation.Start
04/17/2025 3:10 PM	WSP	Start	Starting: Make Address Transaction call to CVAD broker	BrokerGetAddressCall.Start
04/17/2025 3:10 PM	WSP	Start	Starting: Getting cached or fresh resource information for resource id	GetResourceInformation.Start
04/17/2025 3:10 PM	WSP	Start	Starting: Store LaunchIca endpoint API call	StoreLaunchIcaEndpoint.Start
04/17/2025 3:10 PM	WSP	End	Successfully completed: FAS is configured, attempting to retrieve addre...	GetVdaResourceLocation.End
04/17/2025 3:10 PM	WSP	End	Successfully completed: Make Address Transaction call to CVAD broker	BrokerGetAddressCall.End
04/17/2025 3:10 PM	WSP	End	Successfully completed: Store LaunchIca endpoint API call Warnings: Er...	StoreLaunchIcaEndpoint.End

Código de erro

Agente do Broker

bka.prepare.session.failure.validation

- Descrição: Falha ao validar a solicitação de preparação da sessão.
- Ação Recomendada: Tente novamente. Se a falha se repetir, verifique se os conectores estão em um estado saudável.

bka.prepare.session.failure.rejected

- Descrição: O VDA não pode aceitar a solicitação de inicialização.
- Ação Recomendada: Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.

bka.hdx.prepare.failure.general

- Descrição: Falha na preparação do HDX™.
- Ação Recomendada: Reinicie o VDA.

bka.hdx.validate.failure.ticket_not_found

- Descrição: Ticket referenciado ou inicialização não encontrado no cache de inicialização.
- Ação Recomendada: Certifique-se de que o VDA possa se comunicar com o conector.

bka.ticketing.validate.failure.unlicensed

- Descrição: Não é possível verificar a licença para o lançamento.
- Ação Recomendada: Entre em contato com o Suporte Citrix.

bka.ticketing.validate.failure.general

- Descrição: Falha genérica ao validar um tíquete.
- Ação Recomendada: Colete os logs no VDA e entre em contato com o Suporte Citrix.

bka.set.configuration.failure.policy

- Descrição: Ocorreu um erro durante a definição das políticas.
- Ação Recomendada: Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.

bka.set.configuration.failure

- Descrição: Ocorreu um erro durante a definição da configuração.
- Ação Recomendada: Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.

Broker

brk.validate.credentials.failure.invalid

- Descrição: Falha ao validar as credenciais devido a algum problema. A razão pode ser expandida no parâmetro da mensagem.
- Ação Recomendada: Tente a ação novamente. Se a falha se repetir, verifique se os conectores estão em um estado saudável.

brk.resolve.machine.failure.general

- Descrição: Falha ao enumerar ou resolver o worker. O motivo pode ser detalhado no parâmetro da mensagem.
- Ação Recomendada: Certifique-se de que as máquinas capazes de iniciar este aplicativo estejam registradas no Broker. Certifique-se de que todas as máquinas disponíveis não atingiram sua capacidade.

brk.license.check.failure.constraints

- Descrição: As restrições de licenciamento impediram o início da sessão.
- Ação Recomendada: Certifique-se de que há licenças disponíveis para este tipo de aplicativo ou desktop.

brk.resolve.machine.failure.timeout

- Descrição: O Broker atingiu o tempo limite ao contatar o banco de dados.
- Ação Recomendada: Problemas de comunicação com o banco de dados do site. Entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.queued.failure.general

- Descrição: Falha ao enfileirar a ação de energia.
- Ação Recomendada: Problemas de comunicação com o banco de dados do site. Entre em contato com o suporte da Citrix.

brk.set.configuration.failure.general

- Descrição: Erro não especificado ao definir a configuração no VDA de destino.
- Ação Recomendada: Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.

brk.prepare.session.failure.host_unreachable

- Descrição: Falha ao comunicar com o VDA.

- Ação Recomendada: Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.

brk.prepare.session.failure.general

- Descrição: Falha ao preparar a sessão no VDA, erros UnsupportedClientType ou ConnectionRefused.
- Ação Recomendada: Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.

brk.validate.ticket.failure.license

- Descrição: Falha ao recuperar uma licença válida para esta sessão.
- Ação Recomendada: Verifique o status de integridade do site e certifique-se de que todos os conectores e o Citrix DDC estejam operacionais.

brk.validate.ticket.failure.general

- Descrição: Chamada de tíquete inválida.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

brk.reverse.prepare.failure.general

- Descrição: Falha genérica durante o lançamento da sessão.
- Ação Recomendada: Verifique o status de integridade do site e certifique-se de que todos os conectores e o Citrix DDC estejam operacionais.

brk.reverse.prepare.failure.lease_revoked

- Descrição: O lease para esta sessão foi revogado.
- Ação Recomendada: Tente a ação novamente; se a falha se repetir, verifique se os conectores estão em um estado saudável.

brk.reverse.prepare.failure.resource_unavailable

- Descrição: O recurso já está em uso ou está temporariamente indisponível.
- Ação Recomendada: Tente a ação novamente; se a falha se repetir, verifique se os conectores estão em um estado saudável.

brk.reverse.prepare.failure.app_protection

- Descrição: A Proteção de Aplicativos está ausente e é necessária para esta sessão.
- Ação Recomendada: Certifique-se de que a proteção de aplicativos esteja habilitada neste VDA ou remova o requisito de Proteção de Aplicativos do aplicativo.

HDX VDA Linux

VDA_LINUX_ERR_RECONNECT_PRE_LOGOFF

- Descrição: Não é permitido reconectar a uma sessão em estado de pré-logoff.
- Ação recomendada: Tente iniciar mais tarde, isso dá tempo para a sessão fazer logoff.

VDA_LINUX_ERR_RECONNECT_NO_SESSION

- Descrição: Reconectar a uma sessão não existente.
- Ação recomendada: Tente iniciar novamente mais tarde. Se ainda falhar, entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_SAME_KEY

- Descrição: Preparar para uma conexão, mas existe uma sessão com a mesma chave de sessão.
- Ação recomendada: Entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_GET_FQDN

- Descrição: Falha ao obter o FQDN deste VDA.
- Ação recomendada: Verifique se a configuração de DNS no VDA está correta

VDA_LINUX_ERR_NO_CGP_LISTENER

- Descrição: Não há um listener CGP em execução.
- Ação recomendada: Verifique se a política **Conexões de confiabilidade da sessão** está ativada. Verifique se o listener CGP está escutando na porta esperada no VDA (a porta padrão é 2598, pode ser alterada através da política **Número da porta de confiabilidade da sessão**).

VDA_LINUX_ERR_DTLS_CONNECT

- Descrição: Falha ao estabelecer uma conexão DTLS com o serviço Gateway.
- Ação recomendada: Verifique se o FQDN do serviço Gateway é acessível a partir do VDA. Verifique se o caminho `/var/xdl/keystore/cacerts` existe no VDA. Remova `/var/xdl/keystore` e execute `/var/xdl/split_ca_bundle.sh` para regenerar os certificados CA. Verifique se o FQDN do serviço Gateway é confiável para o VDA.

VDA_LINUX_ERR_ACCEPT_EDT_CONNECT

- Descrição: Falha ao aceitar o handshake EDT do cliente.

- Ação recomendada: Entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_TCP_CONNECT

- Descrição: Falha ao estabelecer uma conexão TCP com o serviço Gateway.
- Ação recomendada: Verifique se o FQDN do serviço Gateway está acessível a partir do VDA.

VDA_LINUX_ERR_TLS_CONNECT

- Descrição: Falha ao estabelecer um handshake TLS com o serviço Gateway.
- Ação recomendada: Verifique se o caminho `/var/xdl/keystore/cacerts` existe no VDA. Remova `/var/xdl/keystore` e execute `/var/xdl/split_ca_bundle.sh` para regenerar os certificados CA. Verifique se o FQDN do serviço Gateway é confiável.

VDA_LINUX_ERR_RDVZ_HANDSHAKE

- Descrição: Falha ao estabelecer um handshake de rendezvous com o serviço Gateway.
- Ação recomendada: Entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_ACCEPT_ICA_CONNECT

- Descrição: Falha ao aceitar uma conexão ICA®.
- Ação recomendada: Entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_RECONNECT_TO_ANON_SESSION_NOT_ALLOWED

- Descrição: Reconectar a uma sessão anônima não é permitido.
- Ação recomendada: Entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_CONN_NOT_ALLOWED

- Descrição: A conexão não é permitida.
- Ação recomendada: Se o código de resultado for 3, verifique se a licença não expirou; caso contrário, tente iniciar novamente mais tarde. Se não conseguir resolver, entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_CONN_GENERAL

- Descrição: Falha ao validar a conexão.
- Ação recomendada: Entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_USER_CANCELLED_LOGIN

- Descrição: O usuário final cancelou o logon.

- Ação recomendada: Este erro é esperado quando o SSO está desabilitado e o usuário final clica no botão 'Cancelar' na caixa de logon; caso contrário, entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_GET_TARGET

- Descrição: Falha ao obter a sessão de destino.
- Ação recomendada: Entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_START_LOGON_TIMERS

- Descrição: Falha ao iniciar os temporizadores de logon.
- Ação recomendada: Entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_SEND_CMD_TO_TARGET

- Descrição: Falha ao enviar comando para a sessão de destino.
- Ação recomendada: Entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_POST_RECONNECT_EVENT

- Descrição: Falha ao postar um evento de reconexão.
- Ação recomendada: Entre em contato com o suporte da Citrix.

VDA_LINUX_ERR_RECONNECT_TIMEOUT

- Descrição: Tempo limite de reconexão à sessão do usuário.
- Ação recomendada: Entre em contato com o suporte da Citrix.

HDX VDA Windows

RENDEZVOUS_CONNECT_FAILED_TCP

- Descrição: A tentativa de conexão de rendezvous de saída do VDA para o ponto de rendezvous do Citrix Gateway via TCP falhou.
- Ação recomendada:
  - Revisar a configuração de rede de rendezvous e UDP/DTLS no VDA.
  - Abra um tíquete de suporte se tudo o que foi mencionado acima parecer apropriado. Compartilhe rastreamentos AO e CDF do VDA e captura de pacotes de rede do gateway/VDA (se possível).

RENDEZVOUS_CONNECT_FAILED_EDT

- Descrição: A tentativa de conexão de rendezvous de saída do VDA para o ponto de rendezvous do Citrix Gateway via EDT falhou.
- Ação recomendada:
  - Revisar a configuração de rede de rendezvous e UDP/DTLS no VDA e CGS.
  - Abra um tíquete de suporte se tudo o que foi mencionado acima parecer apropriado. Compartilhe rastreamentos AO e CDF do VDA e captura de pacotes de rede do gateway/VDA (se possível).

RENDEZVOUS_CONNECT_FAILED_PROXY

- Descrição: A tentativa de conexão de rendezvous de saída do VDA para o ponto de rendezvous do Citrix Gateway via proxy falhou.
- Ação recomendada:
  - Revise a configuração do proxy de rendezvous em consulta com a documentação da Citrix.
  - Abra um tíquete de suporte se tudo o que foi mencionado acima parecer apropriado. Compartilhe rastreamentos AO e CDF do VDA e captura de pacotes de rede do gateway/VDA (se possível).

RENDEZVOUS_CONNECT_FAILED_DTLS

- Descrição: A tentativa de conexão de rendezvous de saída do VDA para o ponto de rendezvous do Citrix Gateway falhou devido a uma falha no handshake DTLS.
- Ação recomendada:
  - Revise a configuração de rede rendezvous e UDP/DTLS no VDA.
  - Revise os requisitos de rendezvous e criptográficos com base na documentação da Citrix.
  - Abra um tíquete de suporte se tudo o que foi dito acima parecer apropriado. Compartilhe os rastreamentos AO e CDF do VDA e a captura de pacotes de rede do gateway/VDA (se possível).

RENDEZVOUS_CONNECT_FAILED_TLS

- Descrição: A tentativa de conexão rendezvous de saída do VDA para o ponto de rendezvous do Citrix Gateway falhou devido a uma falha no handshake TLS.
- Ação recomendada:

- Revise a configuração de rede rendezvous e TCP/DTLS no VDA.
- Revise os requisitos de rendezvous e criptográficos com base na documentação da Citrix.
- Abra um tíquete de suporte se tudo o que foi dito acima parecer apropriado. Compartilhe os rastreamentos AO e CDF do VDA e a captura de pacotes de rede do gateway/VDA (se possível).

RENDEZVOUS_CONNECT_FAILED_CGP

- Descrição: Uma tentativa de conexão de transporte Rendezvous de saída falhou devido a um problema de configuração do CGP.
- Ação recomendada: Verifique se o CGP (Session Reliability) está ativado e se as portas CGP estão sendo escutadas, entre em contato com o suporte da Citrix.

CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT

- Descrição: O VDA entra em Session Reliability (SR) quando a sessão ICA sofre uma interrupção de rede, causando a interrupção no fluxo de pacotes. Se esse problema de rede não for resolvido dentro de um período especificado (padrão definido para 180 segundos, consulte a documentação da política da Citrix), um tempo limite pode ocorrer, indicado pelo evento CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT.
- Ação recomendada:
  - Se a sessão ICA não se reconectar dentro do período de tempo limite, o usuário final pode revisar a conectividade de rede no cliente, por exemplo, as configurações de rede e internet na barra de tarefas do Windows.
  - Enquanto a sessão ICA estiver no modo de Confiabilidade da Sessão, tente abrir um recurso da internet em um navegador da web no cliente para garantir que o acesso à internet funcione como esperado.
  - Se o site carregar, mas a sessão ICA falhar ao reconectar, é necessária depuração adicional. Abra um tíquete de suporte com os logs AO e, preferencialmente, rastreamentos CDF do VDA e do Cliente.

CGP_SR_SUSPEND_RESUME_FAILED

- Descrição: O VDA entra em Confiabilidade da Sessão (SR) quando a sessão ICA sofre uma interrupção de rede que causa a interrupção no fluxo de pacotes. O evento CGP_SR_SUSPEND_RESUME_FAILED indica que houve uma falha no processamento da solicitação de suspensão ou retomada, diferente de um tempo limite.

- Ação recomendada: Abra um tíquete de suporte com os logs AO e, preferencialmente, rastreamentos CDF, topologia de rede, especialmente o uso de repetidores de filial.

PREPARE_RECONNECT_REJECTED

- Descrição: O VDA rejeitou uma solicitação de reconexão de uma conexão ICA de entrada devido a uma chave de sessão inválida.
- Ação recomendada:
  - Revise os logs de eventos no VDA para erros de criação de ouvinte.
  - Alternativamente, verifique se os ouvintes estão ativos. Em máquinas RDS, 'netstat -a' pode listar as portas e os proprietários correspondentes. Verifique se algum aplicativo já está usando portas designadas para ICA.
  - Abra um tíquete de suporte com a Citrix e inclua os logs AO e, preferencialmente, rastreamentos CDF para todos os módulos no cliente e no VDA.

Erro: PREPARE_REJECTED

- Descrição: O VDA rejeitou uma solicitação de conexão de uma conexão ICA de entrada devido a uma chave de sessão inválida.
- Ação recomendada: Verifique a configuração do VDA, entre em contato com o suporte da Citrix.

PREPARE_LISTENING_FAILED

- Descrição: O VDA falhou ao iniciar os listeners para a conexão ICA de entrada.
- Ação recomendada: Verifique a configuração de rede, verifique se as portas do listener não estão em uso por outros aplicativos, entre em contato com o suporte da Citrix.

RENDEZVOUSCONNECTIONREQ_FAILED

- Descrição: O VDA falhou ao notificar a pilha ICA para iniciar uma conexão Rendezvous de saída.
- Ação recomendada: Verifique a configuração do rendezvous, verifique a configuração do proxy rendezvous, verifique a configuração do CGP (Confiabilidade da Sessão), entre em contato com o suporte da Citrix.

RENDEZVOUSCONNECTIONREQ_FAILED_PROXYCONFIG

- Descrição: O VDA falhou ao solicitar à pilha ICA para iniciar uma conexão Rendezvous de saída devido a um erro de configuração de proxy.

- Ação recomendada: Verifique a configuração do proxy rendezvous, entre em contato com o suporte da Citrix.

ESTABLISH_SESSION_FAILED

- Descrição: O VDA falhou ao criar uma sessão para a conexão ICA de entrada ou falhou ao se conectar a uma sessão existente.
- Ação recomendada: Abra um tíquete de suporte com os logs do AO e, preferencialmente, rastreamentos CDF para todos os módulos no cliente e no VDA.

ICA_ESTABLISH_FAILED

- Descrição: Uma conexão de transporte é recebida, mas o estabelecimento da conexão falha durante o handshake.
- Ação recomendada:
  - Revise o software de varredura de portas que verifica portas ICA como 1494, 2598, que podem ter ouvintes sempre ativados para receber qualquer solicitação de conexão e, portanto, podem gerar essas mensagens como tentativas falhas. Ou filtre os erros no splunk que não possuem sequência de pré-lançamento necessária para a sessão ICA.
  - Abra um tíquete de suporte com os logs AO e, preferencialmente, rastreamentos CDF, capturas do Wireshark (se possível) do VDA e do Cliente para outras falhas.

VALIDATE_FAILED

- Descrição: O Broker falhou ao validar uma solicitação de conexão ICA de entrada do VDA.
- Ação recomendada: Abra um tíquete de suporte com os logs AO e, preferencialmente, rastreamentos CDF para todos os módulos no cliente e no VDA.

VALIDATE_TICKETING_FAILED

- Descrição: O Broker falhou ao validar uma solicitação de conexão ICA de entrada do VDA devido a um problema de tíquete.
- Ação recomendada: Abra um tíquete de suporte com os logs AO e, preferencialmente, rastreamentos CDF para todos os módulos no cliente e no VDA.

PREPARE_FAILED

- Descrição: Geralmente significa que a preparação para a sessão ICA de entrada falhou no VDA devido a algum erro.
- Ação recomendada:

- Revise o estado da sessão no Citrix Studio para confirmar que as sessões foram encerradas e não estão persistindo.
- Verifique se os ouvintes foram iniciados. Revise o visualizador de eventos no VDA para erros de criação de ouvinte.
- Abra um tíquete de suporte com a Citrix e inclua os logs AO e, preferencialmente, rastreamentos CDF para todos os módulos no cliente e no VDA.

MCS

brk.poweron.forlaunch.execution.generalfailure

- Descrição: Erros gerais.
- Ação recomendada: Entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.insufficientresourcefailure

- Descrição: Uma operação de hipervisor não pode ser concluída devido a recursos insuficientes no hipervisor.
- Ação recomendada: Verifique a cota de recursos no hipervisor. Se não conseguir encontrar uma solução, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.nosuchmanagedmachine

- Descrição: Um ID de máquina não existe.
- Ação recomendada: Verifique o ID da máquina no hipervisor. Se não conseguir encontrar uma solução, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.hypervisorconnectionfailure

- Descrição: Não foi possível estabelecer uma conexão com o hipervisor. Por exemplo, o endereço da infraestrutura de hospedagem não foi encontrado.
- Ação recomendada: Verifique se o endereço da infraestrutura de hospedagem está correto. Se não conseguir encontrar uma solução, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.invalidcredentialsfailure

- Descrição: Credenciais inválidas.
- Ação recomendada: Verifique as credenciais para a conexão do hipervisor. Se não conseguir encontrar uma solução, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.authorizationfailure

- Descrição: Privilégio ou credenciais insuficientes.
- Ação recomendada: Verifique a permissão atribuída às credenciais para a conexão do hipervisor. Se não conseguir encontrar uma solução, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.sslcertauthfailure

- Descrição: Não é possível estabelecer uma conexão devido a um problema de autenticação SSL.
- Ação recomendada: Verifique o certificado de conexão do hipervisor. Se não conseguir encontrar uma solução, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.ratelimitedfailure

- Descrição: A conexão com a nuvem informa que está aplicando limitação de taxa.
- Ação recomendada: Tente a conexão novamente mais tarde se a solicitação for bloqueada pela limitação de taxa do hipervisor. Se não conseguir encontrar uma solução, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.connectorconnectionfailure

- Descrição: Existem erros no conector de nuvem. Por exemplo, ocorre um tempo limite enquanto se aguarda a conexão. Uma vez atingido o tempo limite, o conector de nuvem é desconectado.
- Ação recomendada: Reinicie o conector de nuvem. Se isso falhar, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.remotehclserverconnectionfailure

- Descrição: Erros no plug-in HCL/proxy remoto ou no ponto de extremidade não foram encontrados ao configurar a conexão com o plug-in.
- Ação recomendada: Reinicie o conector. Se isso falhar, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.expiredcredentialsfailure

- Descrição: Uma credencial expirada foi fornecida.
- Ação recomendada: Atualize as credenciais expiradas usadas pela conexão do hipervisor.

brk.poweron.forlaunch.execution.mcsmachinemanagementcustomfailure

- Descrição: Erros durante a criação da máquina.

- Ação recomendada: Entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.detachdiskfailed

- Descrição: A desanexação do disco usado pela máquina virtual falhou.
- Ação recomendada: Entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.createclonefailed

- Descrição: A criação do disco clone falhou no hipervisor.
- Ação recomendada: Entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.provisionedvmnotfound

- Descrição: A VM provisionada não foi encontrada.
- Ação recomendada: Remova a VM provisionada do catálogo. Se isso falhar, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.invalidvmstate

- Descrição: A operação não pode prosseguir devido a um estado de VM inválido.
- Ação recomendada: Reinicie a VM primeiro e tente a operação novamente.

brk.poweron.forlaunch.execution.insufficientresources

- Descrição: Recursos insuficientes durante a operação.
- Ação recomendada: Verifique a cota de recursos utilizada pelo hipervisor.

brk.poweron.forlaunch.execution.hypervisorinmaintenancemode

- Descrição: A operação não pode prosseguir porque o hipervisor está em modo de manutenção.
- Ação recomendada: Verifique se o hipervisor está em modo de manutenção.

brk.poweron.forlaunch.execution.delayed

- Descrição: A operação está na fila.
- Ação recomendada: Aguarde a conclusão do processo. Se a operação falhar, entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.recreatevmfailed

- Descrição: A recriação da VM falhou.
- Ação recomendada: Entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.unknownvirtualmachine

- Descrição: Máquina virtual desconhecida.
- Ação recomendada: Entre em contato com o suporte da Citrix.

brk.poweron.forlaunch.execution.ratelimitexceed

- Descrição: A conexão com a nuvem está limitando a taxa.
- Ação recomendada: Tente a conexão novamente mais tarde se a solicitação foi bloqueada pela limitação de taxa do hypervisor.

brk.poweron.forlaunch.execution.virtualdisknotyetonstorage

- Descrição: O disco virtual não está armazenado.
- Ação recomendada: Tente novamente mais tarde. Se isso falhar, entre em contato com o suporte da Citrix.

Gerenciamento de Perfis

xendesktop.upm.userprofile.error.failure

- Descrição: O Citrix Profile Management falhou ao processar o perfil do usuário. Use um perfil temporário em vez disso.
- Ação recomendada: Este erro não causa uma falha de logon. O Citrix Profile Management usa um perfil temporário em vez disso. Para solucionar o erro, verifique os logs de Eventos do Windows.

xendesktop.upm.userprofile.error.timeout

- Descrição: O Citrix Profile Management falhou ao processar o perfil do usuário dentro do tempo especificado.
- Ação recomendada: Este erro não causa uma falha de logon. O Citrix Profile Management continua processando o perfil do usuário. Para solucionar o erro, verifique os logs do Citrix Profile Management.

Agente WEM

wem.agent.userpolicy.error.failure

- Descrição: O agente do Workspace Environment Management™ (WEM) falhou ao processar as políticas de grupo para o usuário. O logon do usuário continua.

- Ação recomendada: O erro não causa falhas de logon. Para obter mais detalhes, consulte a documentação do produto WEM e verifique os logs do serviço do agente WEM.

wem.agent.userpolicy.error.timeout

- Descrição: O agente do Workspace Environment Management (WEM) falhou ao processar as políticas de grupo para o usuário dentro do tempo especificado. O logon do usuário continua.
- Ação recomendada: O erro não causa falhas de logon. Para obter mais detalhes, consulte a documentação do produto WEM e verifique os logs do serviço do agente WEM.

Pós-lançamento do Android

SessionManager.Launch.EngineLoadFailed

- Descrição: Falha ao carregar ou inicializar o ICA Engine.
- Ação recomendada: Entre em contato com o suporte da Citrix.

SessionManager.Launch.ConnectionFailed

- Descrição: O Engine foi encerrado antes de conectar.
- Ação recomendada: Entre em contato com o suporte da Citrix.

SessionManager.Launch.LogonFailed

- Descrição: A sessão foi desconectada sem concluir o login.
- Ação recomendada: Entre em contato com o suporte da Citrix.

SessionManager.LeaseResolution.Failed

- Descrição: Não foi possível tentar iniciar o lease.
- Ação recomendada: Entre em contato com o suporte da Citrix.

SessionManager.clxmtp.SoftDeny

- Descrição: A negociação CLXMTP do mecanismo falhou (negação suave).
- Ação recomendada: Entre em contato com o suporte da Citrix.

SessionManager.clxmtp.SoftDeny_Implicit

- Descrição: A conexão CLXMTP do mecanismo falhou (negação suave implícita).
- Ação recomendada: Entre em contato com o suporte da Citrix.

Transport.Connect.NoCGP_Fail

- Descrição: Falha ao conectar (CGP desabilitado).
- Ação recomendada: Entre em contato com o suporte da Citrix.

Transport.Connect.FallbackFail

- Descrição: Falha ao conectar. Tentou o fallback ICA.
- Ação Recomendada: Entre em contato com o suporte Citrix.

Transport.Connect.Fail

- Descrição: A conexão está indisponível.
- Ação Recomendada: Entre em contato com o suporte Citrix.

Pré-lançamento do Android

CWA-ICADOWNLOAD_ERR_00001

- Descrição: O tipo de solicitação ICA de envio está incorreto.
- Ação recomendada: Entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00002

- Descrição: A solicitação ICA é inválida.
- Ação Recomendada: Entre em contato com o suporte Citrix.

CWA-ICADOWNLOAD_ERR_00003

- Descrição: O armazenamento é nulo para a solicitação ICA.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00004

- Descrição: A URL da loja é nula para a solicitação ICA.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00005

- Descrição: O parâmetro de recurso é nulo para a solicitação ICA.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00006

- Descrição: O parâmetro de recurso fornecido para a solicitação ICA não é um tipo de recurso válido.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00007

- Descrição: O parâmetro de recurso fornecido para a solicitação ICA é nulo para a URL de inicialização ICA.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00008

- Descrição: A solicitação ICA é nula com parâmetros do gerenciador de autenticação.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00009

- Descrição: O corpo da solicitação ICA é nulo.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00010

- Descrição: Falha ao criar uma entidade HTTP a partir do corpo da solicitação ICA.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00011

- Descrição: Falha ao baixar o arquivo ICA devido a uma exceção ao criar a solicitação do gerenciador de autenticação.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00012

- Descrição: Falha ao baixar o arquivo ICA devido a uma exceção ao executar a solicitação do gerenciador de autenticação.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00013

- Descrição: Falha ao baixar o arquivo ICA devido a uma resposta inesperada da solicitação do gerenciador de autenticação.

- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00014

- Descrição: Falha ao baixar o arquivo ICA ao copiar o inputStream da resposta do gerenciador de autenticação.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00015

- Descrição: Falha ao analisar o documento ICA usando o inputStream da resposta do gerenciador de autenticação.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00016

- Descrição: O documento ICA baixado é nulo sem nenhuma exceção.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00017

- Descrição: Falha ao baixar o arquivo ICA devido a uma resposta malsucedida.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00018

- Descrição: O recurso está indisponível.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00019

- Descrição: O recurso a ser iniciado não existe, não está habilitado ou não está visível para um usuário.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00020

- Descrição: Não há mais sessões ativas.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00021

- Descrição: O servidor não possui a licença necessária para realizar a atividade solicitada.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00022

- Descrição: Não há estações de trabalho disponíveis.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00023

- Descrição: Não é possível conectar à estação de trabalho. O servidor recusou a conexão.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00024

- Descrição: A estação de trabalho está em manutenção e não está disponível para uso.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00025

- Descrição: Não é possível iniciar o recurso devido a um erro `resourceerror` no arquivo ICA.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00026

- Descrição: Não é possível iniciar o recurso devido a um erro `generalapplauncherror` no arquivo ICA.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00027

- Descrição: Não é possível iniciar o recurso devido a um erro desconhecido no arquivo ICA.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00028

- Descrição: Não é possível iniciar o recurso devido a um erro de reinicialização no arquivo ICA.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00029

- Descrição: Não é possível iniciar o recurso devido a um erro de retomada no arquivo ICA.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00030

- Descrição: Não é possível iniciar o recurso devido a um erro indefinido no arquivo ICA.

- Ação Recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00031

- Descrição: Não é possível baixar o arquivo ICA. No entanto, o código de erro não foi encontrado no mapa definido.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

Pós-lançamento do Linux

SessionManager.Launch.EngineLoadFailed

- Descrição: Falha ao carregar o mecanismo ICA.
- Ação recomendada: Entre em contato com o suporte da Citrix.

SessionManager.Launch.Failed

- Descrição: Falha ao iniciar a sessão.
- Ação Recomendada: Entre em contato com o suporte da Citrix.

SessionManager.Launch.ConnectionFailed

- Descrição: O mecanismo foi encerrado antes de conectar.
- Ação Recomendada: Procure por outros erros associados à tentativa de inicialização.

SessionManager.Launch.LogonFailed

- Descrição: A sessão foi desconectada sem concluir o login.
- Ação Recomendada: Este erro indica falha de login, possivelmente incluindo uma falha do usuário ao inserir credenciais manualmente. Investigue como o usuário tentou fazer login no VDA remoto.

SessionManager.LeaseResolution.Failed

- Descrição: Não foi possível tentar iniciar o lease.
- Ação Recomendada: Verifique se os leases foram sincronizados com a máquina cliente e se ainda são válidos. O usuário pode fazer login em sua loja no modo online para acionar a (re-)sincronização dos leases. Procure por erros enviados pelos componentes Gateway ou Cloud Connector. Esses erros podem indicar as razões da falha.

Transport.Connect.NoCGP_Fail

- Descrição: Falha ao conectar (CGP desabilitado).

- Ação Recomendada: Investigue por que o cliente não consegue contatar um VDA via TCP ou EDT.

Transport.Connect.FallbackFail

- Description: Falha ao conectar. Tentou o fallback ICA.
- Recommended Action: Investigue por que o cliente não consegue contatar um Gateway, Connector ou VDA via TCP ou EDT.

Transport.Connect.Fail

- Description: O aplicativo Citrix Workspace falhou ao conectar-se ao Gateway, Connector ou VDA via TCP, EDT ou UDP.
- Recommended Action: Investigue por que o cliente não consegue contatar o Gateway, Connector ou VDA via TCP, EDT ou UDP. O firewall entre o cliente e o host pode não permitir os protocolos (UDP/TCP) ou as portas necessárias.

SessionManager.clxmtp.SoftDeny

- Description: A negociação do Engine CLXMTP falhou (soft deny).
- Recommended Action: Este erro não indica que o lançamento deve falhar. Ele indica que o mecanismo não pode ter sucesso através de um caminho de rede específico. Procure por erros que os componentes do Gateway ou Cloud Connector enviaram. Esses erros podem indicar as razões da falha.

SessionManager.clxmtp.SoftDeny_Implicit

- Description: A conexão do Engine CLXMTP falhou (implicit soft deny).
- Recommended Action: Este erro não indica que o lançamento deve falhar. Ele indica que o mecanismo não pode ter sucesso através de um caminho de rede específico. Investigue por que o cliente não consegue contatar um Connector ou Gateway. Pode ser esperado que esse host esteja inacessível devido à topologia de rede ou restrições de firewall.

Pré-lançamento do Linux

CWA-ICADOWNLOAD_ERR_00001

- Description: Não foi possível conectar à loja devido à falta de resposta do aplicativo Citrix Workspace.
- Recommended action: Verifique se o Citrix® StoreFront Cloud ou o Citrix® StoreFront está inativo. Além disso, verifique a conectividade com a internet.

CWA-ICADOWNLOAD_ERR_00002

- Descrição: O usuário cancelou o lançamento da sessão.
- Ação recomendada: Reinicie a sessão depois de algum tempo.

CWA-ICADOWNLOAD_ERR_00003

- Descrição: Não foi possível conectar à loja. Verifique se os certificados do servidor são válidos.
- Ação recomendada: Verifique se os certificados do servidor estão instalados e ativos.

CWA-ICADOWNLOAD_ERR_00004

- Descrição: O recurso a ser iniciado não existe, não está habilitado ou não está visível para um usuário.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00005

- Descrição: As estações de trabalho não estão disponíveis para esta solicitação.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00006

- Descrição: O servidor não possui a licença necessária para realizar a atividade solicitada.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00007

- Descrição: O servidor recusou a conexão com a estação de trabalho.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00008

- Descrição: A estação de trabalho solicitada está em manutenção e indisponível para uso.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00009

- Descrição: O limite máximo de sessões foi atingido.
- Ação recomendada: O limite máximo de sessões configurado por um administrador foi atingido. Reinicie a sessão.

CWA-ICADOWNLOAD_ERR_000010

- Descrição: Erro geral que não pode ser especificado com mais detalhes.
- Ação recomendada: Entre em contato com o suporte da Citrix.

Pós-lançamento do Mac

Falha ao iniciar a área de trabalho

- Descrição: Falha ao iniciar a área de trabalho "Nome da área de trabalho". ID da transação - "ID da transação".
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

O visualizador falhou ao iniciar

- Descrição: O visualizador falhou ao iniciar. ID da transação - "ID da transação".
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

A área de trabalho falhou ao iniciar

- Descrição: A área de trabalho "Nome da área de trabalho" está em manutenção planejada. ID da transação - "ID da transação".
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

O aplicativo falhou ao iniciar

- Descrição: O aplicativo "Nome do aplicativo" falhou ao iniciar.
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

O aplicativo falhou ao iniciar

- Descrição: O aplicativo "Nome do aplicativo" falhou ao iniciar. ID da transação - "ID da transação".
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

A área de trabalho falhou ao iniciar

- Descrição: A área de trabalho "Nome da área de trabalho" falhou ao iniciar.
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

Falha ao iniciar o desktop

- Descrição: Falha ao iniciar o desktop "Nome do desktop". ID da transação - "ID da transação".
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

Falha ao iniciar o Visualizador

- Descrição: Falha do Visualizador ao abrir "Nome do aplicativo". ID da transação - "ID da transação".
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

Falha ao iniciar o Visualizador

- Descrição: Falha do Visualizador ao abrir o desktop "Nome do desktop". ID da transação - "ID da transação".
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

Falha ao iniciar o desktop

- Descrição: O desktop "Nome do desktop" está em manutenção programada.
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

Falha ao iniciar o desktop

- Descrição: O desktop "Nome do desktop" está em manutenção programada. ID da transação - "ID da transação".
- Ação recomendada: Entre em contato com seu administrador com os detalhes do erro.

Não é possível conectar-se à área de trabalho

- Descrição: Não é possível acessar a área de trabalho "nome da área de trabalho". ID da transação - "ID da transação". Tente novamente mais tarde.
- Ação recomendada: Se o problema persistir, entre em contato com seu administrador com os detalhes do erro.

Pré-lançamento do Mac

CWA-ICADOWNLOAD_ERR_00001

- Descrição: O arquivo ICA é inválido.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00002

- Descrição: A solicitação de inicialização expirou.
- Ação recomendada: Verifique a conexão com a internet ou entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00003

- Descrição: O servidor não respondeu.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00004

- Descrição: O recurso a ser iniciado não existe, não está habilitado ou não está visível para o usuário.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00005

- Descrição: O servidor não está acessível.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00006

- Descrição: Erro ao iniciar o visualizador.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00007

- Descrição: Falha ao iniciar um evento de abertura da Apple.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00008

- Descrição: O caminho do visualizador não está acessível.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CWA-ICADOWNLOAD_ERR_00009

- Descrição: O usuário cancelou a autenticação.
- Ação recomendada: Peça ao usuário para reiniciar o recurso.

CWA-ICADOWNLOAD_ERR_000010

- Descrição: O usuário cancelou a janela LSI.
- Ação recomendada: Peça ao usuário para reiniciar o recurso.

CWA-ICADOWNLOAD_ERR_000011

- Descrição: A estação de trabalho solicitada está em manutenção e indisponível para uso.

- Ação recomendada: Peça ao usuário para tentar novamente após a conclusão da manutenção e quando a estação de trabalho estiver disponível para uso.

CWA-ICADOWNLOAD_ERR_000012

- Descrição: As credenciais de login do usuário devem ser alteradas.
- Ação recomendada: Peça ao usuário para alterar as credenciais de login.

CWA-ICADOWNLOAD_ERR_000013

- Descrição: A sessão que conecta o recurso não está mais ativa.
- Ação recomendada: Peça ao usuário para tentar novamente ou entre em contato com o suporte técnico da Citrix para obter assistência adicional.

CWA-ICADOWNLOAD_ERR_000014

- Descrição: Falha ao baixar o arquivo ICA.
- Ação recomendada: Entre em contato com o suporte da Citrix.

Pós-lançamento do Windows

SessionManager.Launch.EngineLoadFailed

- Descrição: Os componentes principais para estabelecer uma conexão com uma área de trabalho ou aplicativo remoto falharam ao carregar ou inicializar corretamente. Detalhes adicionais podem ser fornecidos na mensagem de erro.
- Ação recomendada: O aplicativo Citrix Workspace não está funcionando como esperado. Uma DLL de canal virtual de terceiros (não Citrix) ou outro componente do sistema pode estar causando esse problema. Pode ser necessário coletar e enviar rastreamentos CDF para determinar a natureza da falha.

SessionManager.Launch.ConnectionFailed

- Descrição: Este erro é uma falha genérica que indica que uma tentativa de lançamento falhou. Outros erros enviados podem indicar uma causa.
- Ação recomendada: Procure outros erros associados à tentativa de lançamento.

SessionManager.Launch.LogonFailed

- Descrição: Este erro indica que uma conexão com uma área de trabalho ou aplicativo remoto foi estabelecida. No entanto, a sessão foi desconectada sem concluir o login do Windows (ou de outro sistema operacional).

- Ação recomendada: Este erro indica alguma falha de login, possivelmente incluindo uma falha do usuário ao inserir credenciais manualmente. Investigue como o usuário tentou fazer login no VDA remoto.

SessionManager.Launch.Cancelled

- Descrição: A tentativa de conexão do mecanismo Citrix foi cancelada, provavelmente por ação do usuário.
- Ação recomendada: Este erro indica por que uma conexão não foi estabelecida com sucesso, mas provavelmente indica um comportamento correto.

SessionManager.LeaseResolution.Failed

- Description: Indica que uma inicialização offline (também chamada de "baseada em lease") falhou. Essa falha ocorre porque um lease válido e necessário para o recurso não foi encontrado na máquina cliente. Além disso, o Gateway ou Cloud Connector rejeitou a solicitação de inicialização, ou a solicitação de inicialização era de alguma forma inválida.
- Ação recomendada: Verifique se os leases foram sincronizados com a máquina cliente e se ainda são válidos. O usuário pode fazer login em sua loja no modo online para acionar a (re-)sincronização dos leases. Procure os erros que os componentes do Gateway ou Cloud Connector enviaram. Esses erros podem indicar as razões da falha.

SessionManager.clxmtp.SoftDeny

- Description: Uma inicialização de lease foi tentada, e um Connector ou Gateway informou ao cliente que não pode concluir a inicialização solicitada. No entanto, os outros Connectors ou Gateways podem ser capazes de ajudar na inicialização.
- Ação recomendada: Este erro não indica que a inicialização deve falhar. Ele indica que o motor não pode ter sucesso através de um caminho de rede específico. Procure os erros que os componentes do Gateway ou Cloud Connector enviaram. Esses erros podem indicar as razões da falha.

SessionManager.clxmtp.SoftDeny_Implicit

- Description: Uma inicialização de lease foi tentada, e um Connector ou Gateway estava inacessível. No entanto, outros Connectors ou Gateways podem ser capazes de ajudar na inicialização.
- Ação recomendada: Este erro não indica que a inicialização deve falhar. Ele indica que o motor não pode ter sucesso através de um caminho de rede específico. Investigue por que o cliente não consegue contatar um Connector ou Gateway. Pode ser esperado que esse host esteja inacessível devido à topologia de rede ou restrições de firewall.

Transport.Connect.NoCGP_Fail

- Description: Os componentes principais (motor) do aplicativo Citrix Workspace falharam ao se conectar a um host VDA através do protocolo ICA (porta 1494). Tentativas de conexão a um gateway ou VDA via protocolo CGP não foram realizadas se este evento foi enviado.
- Ação recomendada: Investigue por que o cliente não consegue contatar um VDA via TCP ou EDT.

Transport.Connect.FallbackFail

- Description: Os componentes principais (motor) do aplicativo Citrix Workspace falharam ao se conectar a um host VDA através do protocolo ICA (porta 1494). Após essa falha, o aplicativo Citrix Workspace falha ao se conectar a um Gateway ou VDA através do protocolo CGP (porta 2598).
- Ação recomendada: Investigue por que o cliente não consegue contatar um Gateway, Connector ou VDA via TCP ou EDT.

Transport.Connect.Fail

- Descrição: Os componentes principais (mecanismo) do aplicativo Citrix Workspace falharam ao se conectar a um Gateway ou VDA através do protocolo CGP (porta 2598). Tentativas de conexão a um VDA através do protocolo ICA não foram realizadas se este evento foi emitido.
- Ação recomendada: Investigue por que o cliente não consegue contatar um Gateway, Connector ou VDA via TCP ou EDT.

Pré-lançamento do Windows

CWA-ICADOWNLOAD_ERR_00001

- Descrição: Não foi possível conectar à loja devido à falta de resposta do aplicativo Citrix Workspace.
- Ação recomendada: Verifique se o Citrix® StoreFront Cloud ou o Citrix StoreFront está inativo. Além disso, verifique a conectividade com a internet.

CWA-ICADOWNLOAD_ERR_00002

- Descrição: O usuário cancelou o lançamento da sessão.
- Ação recomendada: Reinicie a sessão depois de algum tempo.

CWA-ICADOWNLOAD_ERR_00003

- Descrição: Não foi possível conectar à loja. Verifique se os certificados do servidor são válidos.

- Ação recomendada: Entre em contato com o administrador de TI com os detalhes do erro.

CWA-ICADOWNLOAD_ERR_00004

- Descrição: O recurso a ser iniciado não existe, não está habilitado ou não está visível para um usuário.
- Ação recomendada: Entre em contato com o administrador de TI com os detalhes do erro.

CWA-ICADOWNLOAD_ERR_00005

- Descrição: As estações de trabalho não estão disponíveis para esta solicitação.
- Ação recomendada: Entre em contato com o administrador de TI com os detalhes do erro.

CWA-ICADOWNLOAD_ERR_00006

- Descrição: O servidor não possui a licença necessária para realizar a atividade solicitada.
- Ação recomendada: Entre em contato com o administrador de TI com os detalhes do erro.

CWA-ICADOWNLOAD_ERR_00007

- Descrição: O servidor recusou a conexão com a estação de trabalho.
- Ação recomendada: Entre em contato com o administrador de TI com os detalhes do erro.

CWA-ICADOWNLOAD_ERR_00008

- Descrição: A estação de trabalho solicitada está em manutenção e indisponível para uso.
- Ação recomendada: Entre em contato com o administrador de TI com os detalhes do erro.

CWA-ICADOWNLOAD_ERR_00009

- Descrição: O limite máximo de sessões foi atingido.
- Ação recomendada: Atingido o limite máximo de sessões configurado por um administrador. Reinicie a sessão.

CWA-ICADOWNLOAD_ERR_000010

- Descrição: Erro geral que não pode ser especificado em mais detalhes.
- Ação recomendada: Entre em contato com o administrador de TI com os detalhes do erro.

Workspace

StoreLaunchIcaEndpoint.LaunchFailed

- Descrição: Ocorreu um erro durante o lançamento.

- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte da Citrix.

StoreLaunchSessionEndpoint.BadRequest

- Descrição: Os parâmetros da solicitação de lançamento eram inválidos ou vazios.
- Ação recomendada: Entre em contato com o suporte da Citrix.

StoreLaunchSessionEndpoint.FarmUnavailable

- Descrição: Não havia farms disponíveis para o lançamento.
- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops.

StoreLaunchSessionEndpoint.Error

- Description: Houve um erro interno durante o lançamento.
- Recommended action: Entre em contato com o suporte da Citrix.

StoreGetIcaFileEndpoint.BadRequest

- Description: Nenhum tíquete de lançamento foi fornecido na solicitação.
- Recommended action: Entre em contato com o suporte da Citrix.

StoreGetIcaFileEndpoint.RetrieveIcaFileForTicketFailed

- Description: O Workspace não conseguiu recuperar o arquivo ICA.
- Recommended action: Entre em contato com o suporte da Citrix.

StoreGetIcaFileEndpoint.Error

- Description: O Workspace não conseguiu recuperar o arquivo ICA.
- Recommended action: Entre em contato com o suporte da Citrix.

WebProxyGetLaunchStatusEndPoint.DSAuthFailure

- Description: Houve um problema de autenticação.
- Recommended action: Tente reautenticar. Entre em contato com o suporte da Citrix.

WebProxyGetLaunchStatusEndPoint.LaunchFailed

- Descrição: Ocorreu um erro interno ao iniciar o aplicativo.
- Ação recomendada: Entre em contato com o suporte da Citrix.

WebProxyGetLaunchStatusEndPoint.ResourceNotFound

- Descrição: A inicialização falhou porque o aplicativo não pôde ser encontrado.
- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops e a configuração do aplicativo.

WebProxyLaunchIcaEndpoint.DSAuthFailure

- Descrição: Houve um problema de autenticação.
- Ação recomendada: Tente reautenticar. Entre em contato com o suporte da Citrix.

WebProxyLaunchIcaEndpoint.LaunchFailed

- Descrição: Ocorreu um erro interno ao iniciar o aplicativo.
- Ação recomendada: Entre em contato com o suporte da Citrix.

WebProxyLaunchIcaEndpoint.ResourceNotFound

- Descrição: A inicialização falhou porque o aplicativo não pôde ser encontrado.
- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops e a configuração do aplicativo.

WebProxySessionsLaunchIcaEndpoint.SessionNotFound

- Descrição: O Workspace não conseguiu se reconectar à sessão HDX existente. Sua sessão pode ter sido encerrada.
- Ação recomendada: Reinicie o aplicativo.

WebProxySessionsLaunchIcaEndpoint.DSAuthFailure

- Descrição: Houve um problema de autenticação.
- Ação recomendada: Tente se autenticar novamente. Entre em contato com o suporte da Citrix.

WebProxySessionsLaunchIcaEndpoint.ReconnectSessionFailed

- Descrição: O Workspace não conseguiu se reconectar à sessão HDX existente. Sua sessão pode ter sido encerrada.
- Ação recomendada: Entre em contato com o suporte da Citrix.

WebProxySessionsLaunchIcaEndpoint.Error

- Descrição: Ocorreu um erro interno ao tentar se reconectar à sessão.
- Ação recomendada: Entre em contato com o suporte da Citrix.

WebProxySessionsGetLaunchStatusEndpoint.DSAuthFailure

- Descrição: Houve um problema de autenticação.
- Ação recomendada: Tente se autenticar novamente. Entre em contato com o suporte da Citrix.

WebProxySessionsGetLaunchStatusEndpoint.ReconnectSessionFailed

- Descrição: O Workspace não conseguiu se reconectar à sessão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

WebProxySessionsGetLaunchStatusEndpoint.Error

- Descrição: Ocorreu um erro interno ao tentar se reconectar à sessão.
- Ação recomendada: Entre em contato com o suporte da Citrix.

DetermineGateway.Error

- Descrição: O Workspace não conseguiu determinar a qual Gateway se conectar.
- Ação recomendada: Verifique sua configuração do Gateway. Entre em contato com o suporte da Citrix.

ConnectionRoutingProviderLaunch.Error

- Descrição: O Workspace não conseguiu determinar a qual Gateway se conectar.
- Ação recomendada: Verifique sua configuração do Gateway. Entre em contato com o suporte da Citrix.

BrokerGetAddressCall.AnonymousPrelaunchNotSupported

- Descrição: O Workspace não pode iniciar o aplicativo porque o farm não oferece suporte a inicializações anônimas.
- Ação recomendada: Entre em contato com o suporte da Citrix.

BrokerGetAddressCall.LeasingError

- Descrição: O Workspace recebeu um erro do broker do Citrix Virtual Apps and Desktops.
- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte da Citrix.

BrokerGetAddressCall.ServiceConnectionError

- Descrição: O Workspace não conseguiu contatar nenhum broker do Citrix Virtual Apps and Desktops no farm.

- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte da Citrix.

BrokerGetAddressCall.BrokerError

- Descrição: O Workspace recebeu um erro de um broker do Citrix Virtual Apps and Desktops.
- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte da Citrix.

BrokerGetAddressCall.LicensingError

- Descrição: O Workspace não conseguiu iniciar o aplicativo devido a um erro de licenciamento.
- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte da Citrix.

BrokerGetAddressCall.Error

- Descrição: O Workspace não consegue recuperar os detalhes do VDA do broker do Citrix Virtual Apps and Desktops.
- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte da Citrix.

GetLaunchReference.NoAccessToken

- Descrição: O Workspace não consegue se conectar com sucesso ao VDA.
- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte da Citrix.

GetLaunchReference.BrokerError

- Descrição: O Workspace não consegue se conectar com sucesso ao VDA.
- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte da Citrix.

GetLaunchReference.Error

- Descrição: O Workspace não consegue se conectar com sucesso ao VDA.
- Ação recomendada: Verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte da Citrix.

GenerateIcaFile.InvalidIcaSetting

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.

- Ação recomendada: Entre em contato com o suporte da Citrix.

StoreIcaFileAndGetTicket.StoreIcaFileAndCreateTicketFailed

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

StoreIcaFileAndGetTicket.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GetFasVdaLogonTicket.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GenerateSTATicket.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GetVdaAddress.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GetTicket.NoAccessToken

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GetTicket.BrokerError

- Description: O broker do Citrix Virtual Apps and Desktops não conseguiu iniciar a sessão HDX.
- Recommended action: Verifique o ID na mensagem de erro e verifique seus logs do Citrix Virtual Apps and Desktops.

GetTicket.ServiceConnectionError

- Description: O Workspace não consegue contatar um broker do Citrix Virtual Apps and Desktops.
- Recommended action: Entre em contato com o suporte da Citrix.

GetTicket.Error

- Description: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Recommended action: Entre em contato com o suporte da Citrix.

GetNetscalerConfigurationByCustomer.Error

- Description: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Recommended action: Entre em contato com o suporte da Citrix.

DiscoverMPSServerCapabilities.Error

- Description: Houve um problema ao fazer uma solicitação ao broker do Citrix Virtual Apps and Desktops.
- Recommended action: Verifique seus logs do Citrix Virtual Apps and Desktops. Entre em contato com o suporte da Citrix.

GetResourceLocationNetScalerConfig.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GetCustomerResourceLocations.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GetResourceLocationFromResourceProvider.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GetNetScalerGatewayInfo.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GetCustomerEntitlements.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GetResourceLocationForServerFeed.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

GetResourceInformation.Error

- Descrição: Ocorreu um erro interno ao estabelecer uma conexão HDX.
- Ação recomendada: Entre em contato com o suporte da Citrix.

Citrix Gateway como serviço

CGS-ICASN_ERR_00001

- Descrição: Falha no lançamento do aplicativo devido a um erro de análise da solicitação.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00002

- Descrição: Falha ao validar o tíquete de autenticação.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00003

- Descrição: O arquivo ICA baixado do navegador é usado para o lançamento da sessão após 90 segundos, quando o tíquete STA expira.
- Ação recomendada: Tente novamente o lançamento da sessão.

CGS-ICASN_ERR_00004

- Descrição: Falha ao validar o tíquete de autenticação.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00005

- Descrição: Falha ao estabelecer conexão com o Conector.
- Ação recomendada: Verifique a integridade do conector. Se o problema persistir, entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00006

- Descrição: A solicitação de conexão com o Conector expirou.

- Ação recomendada: Verifique a integridade do conector. Verifique se alguma configuração de proxy está bloqueando o tráfego entre o conector/VDA e o NGS. Verifique a conectividade entre o VDA e o Conector. Se o problema persistir, entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00007

- Descrição: A conexão foi fechada pelo aplicativo Citrix Workspace na Máquina Cliente antes que a sessão fosse estabelecida.
- Ação recomendada: Tente iniciar a sessão novamente.

CGS-ICASN_ERR_00008

- Descrição: O back-end fechou a conexão.
- Ação recomendada: Verifique a integridade do conector. Verifique a estabilidade da rede do Conector/VDA para a rede pública (NGS). Se o problema persistir, entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00009

- Descrição: Falha no estabelecimento da conexão VDA para NGS (Rendezvous).
- Ação recomendada: Verifique a integridade do conector. O VDA deve ser capaz de alcançar o Serviço NGS. Verifique a conectividade entre o VDA e o Conector. Se o problema persistir, entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00010

- Descrição: Fallback de EDT para TCP. Verifique o pré-requisito para EDT.
- Ação recomendada: O Rendezvous deve estar habilitado e o VDA deve ser capaz de alcançar o serviço NGS via UDP. Se o problema persistir, entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00011

- Descrição: Falha no serviço interno do NGS.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00012

- Descrição: Falha no serviço interno do NGS.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00013

- Descrição: Falha na validação GCT.

- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00014

- Descrição: Falha na validação GCT.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00015

- Descrição: Falha no serviço interno NGS.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00016

- Descrição: Falha no serviço interno NGS.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00017

- Descrição: Falha no serviço interno NGS.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00018

- Descrição: Falha ao validar o tíquete de autenticação.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00019

- Descrição: Falha ao validar o tíquete de autenticação.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00020

- Descrição: Erro no licenciamento interno do CGS.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00021

- Descrição: Retorno ao Rendezvous v2 devido a um sinalizador de recurso desabilitado.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00022

- Descrição: Falha no serviço interno do NGS.

- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00023

- Descrição: Tempo limite na troca CLXMTP.
- Ação recomendada: Verifique se os conectores estão íntegros e acessíveis ao serviço NGS. Se o problema persistir, entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00024

- Descrição: Falha na validação VSR do CLXMTP.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00025

- Descrição: Falha na validação VSR do CLXMTP.
- Ação recomendada: Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00026

- Descrição: O conector não está disponível no CLXMTP.
- Ação recomendada: Verifique se o conector está em um estado saudável para o local do recurso. Se o problema persistir, entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00027

- Descrição: O redirecionamento do CLXMTP para o Conector falhou após o número máximo de tentativas.
- Ação recomendada: Verifique se o conector está em um estado saudável para o local do recurso. Verifique se o serviço `Citrix ClxMtp Service` está em execução em todos os conectores. Entre em contato com o suporte da Citrix.

CGS-ICASN_ERR_00028

- Descrição: Falha ao se comunicar com o Controller.
- Ação recomendada: Entre em contato com o suporte da Citrix.

Sucesso: CGS_ICASN_SUCCESS_00001

- Descrição: Solicitação de inicialização de sessão recebida.
- Ação recomendada: Não aplicável

Sucesso: CGS_ICASN_SUCCESS_00002

- Descrição: Solicitação de inicialização de sessão concluída.
- Ação recomendada: Não aplicável

Proxy XAXD

XDPXY_INF_00001

- Descrição: O Broker envia uma solicitação ao VDA para se preparar para conexões de entrada.
- Ação recomendada: Não aplicável

XDPXY_INF_00002

- Descrição: O VDA confirma a solicitação de conexão pelo Broker.
- Ação recomendada: Não aplicável

XDPXY_ERR_00001

- Descrição: Falha ao se comunicar com o VDA.
- Ação Recomendada: Verifique a integridade do Connector. Para obter mais informações, consulte Citrix Cloud Connector e CTX224133.
    - Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.
    - Se você tiver um proxy web entre o Connector e o Broker, certifique-se de que ele esteja configurado corretamente.
    - Se o problema persistir, entre em contato com o suporte da Citrix.

XDPXY_ERR_00002

- Descrição: XaxdProxy atingiu o tempo limite esperando uma resposta do VDA.
- Ação Recomendada: Verifique a integridade do Connector. Para obter mais informações, consulte Citrix Cloud Connector e CTX224133.
    - Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.
    - Se você tiver um proxy web entre o Connector e o Broker, certifique-se de que ele esteja configurado corretamente.
    - Se o problema persistir, entre em contato com o suporte da Citrix.

XDPXY_ERR_00003

- Descrição: Foi encontrado um erro ou exceção WCF ao tentar fazer a solicitação.
- Ação Recomendada: Verifique a integridade do Connector. Para obter mais informações, consulte Citrix Cloud Connector e CTX224133.
  - Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.
  - Se você tiver um proxy web entre o Connector e o Broker, certifique-se de que ele esteja configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte da Citrix.

XDPXY_INF_00003

- Descrição: A solicitação de validação para uma conexão ICA ou RDP de entrada é chamada pela pilha.
- Ação recomendada: Não aplicável

XDPXY_INF_00004

- Descrição: A validação da conexão ICA ou RDP de entrada é estabelecida.
- Ação recomendada: Não aplicável

XDPXY_ERR_00001

- Descrição: Falha ao se comunicar com o Proxy VDA.
- Ação recomendada: Verifique a integridade do Connector. Para obter mais informações, consulte Citrix Cloud Connector e CTX224133.
  - Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.
  - Se você tiver um proxy web entre o Connector e o Broker, certifique-se de que ele esteja configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte da Citrix.

XDPXY_ERR_00002

- Descrição: O XaxdProxy atingiu o tempo limite esperando uma resposta do Proxy VDA.
- Ação Recomendada: Verifique a saúde do Connector. Para mais informações, consulte Citrix Cloud Connector e CTX224133.
  - Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.

- Se você tiver um proxy web entre o Connector e o Broker, certifique-se de que ele esteja configurado corretamente.
- Se o problema persistir, entre em contato com o suporte da Citrix.

XDPXY_ERR_00003

- Descrição: Foi encontrada uma exceção ao tentar fazer a solicitação.
- Ação Recomendada: Verifique a saúde do Connector. Para mais informações, consulte Citrix Cloud Connector e CTX224133.
  - Reinicie o serviço Citrix Delivery Agent no VDA ou reinicie o VDA.
  - Se você tiver um proxy web entre o Connector e o Broker, certifique-se de que ele esteja configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte da Citrix.

XDPXY_INF_00005

- Descrição: A solicitação de tráfego de sessão HDX direto para o VDA é feita.
- Ação Recomendada: Não aplicável

XDPXY_INF_00006

- Descrição: O VDA estabelece conexão direta com o plano de controle do Citrix Cloud™ para o tráfego de sessão HDX.
- Ação Recomendada: Não aplicável

XDPXY_INF_00007

- Descrição: O cliente envia uma solicitação de conexão para o StoreFront local para um recurso.
- Ação Recomendada: Não aplicável

XDPXY_INF_00008

- Descrição: O StoreFront local aceita a solicitação de conexão do cliente para o recurso.
- Ação Recomendada: Não aplicável

XDPXY_ERR_00004

- Descrição: O XaxdProxy recebeu uma resposta de erro HTTP ao tentar se conectar.
- Ação Recomendada: Verifique a integridade do Connector. Para obter mais informações, consulte Citrix Cloud Connector e CTX224133.

- Verifique a estabilidade da rede do Connector para a rede pública.
- Se você tiver um proxy web entre o Connector e o Broker, certifique-se de que ele esteja configurado corretamente.
- Se o problema persistir, entre em contato com o suporte da Citrix.

XDPXY_ERR_00006

- Descrição: A solicitação XML tem um formato inválido.
- Ação Recomendada: Entre em contato com o suporte da Citrix

XDPXY_ERR_00007

- Descrição: A solicitação XML tem cabeçalhos de credenciais e/ou formato inválidos.
- Ação Recomendada: Faça logout, faça login novamente e tente a ação. Se o problema persistir, entre em contato com o suporte da Citrix.

XDPXY_INF_00011

- Descrição: O lançamento da continuidade do serviço é solicitado pelo usuário via WSA.
- Ação Recomendada: Não aplicável

XDPXY_INF_00012

- Descrição: O lançamento da continuidade do serviço é solicitado pelo usuário via WSA.
- Ação Recomendada: Não aplicável

XDPXY_ERR_00004

- Descrição: O XaxdProxy encontrou um erro HTTP ao tentar se conectar.
- Ação Recomendada: Verifique a integridade do Connector. Para obter mais informações, consulte Citrix Cloud Connector e CTX224133.
  - Se você tiver um proxy web entre o Connector e o Broker, certifique-se de que ele esteja configurado corretamente.
  - Se o problema persistir, entre em contato com o suporte da Citrix.

XDPXY_ERR_00008

- Descrição: A inicialização da continuidade do serviço falhou porque o XaxdProxy excedeu o tempo limite esperando por uma resposta.
- Ação Recomendada: Verifique a integridade do Connector. Para obter mais informações, consulte Citrix Cloud Connector e CTX224133.

- Se você tiver um proxy web entre o Connector e o Broker, certifique-se de que ele esteja configurado corretamente.
- Se o problema persistir, entre em contato com o suporte da Citrix.

XDPXY_ERR_00009

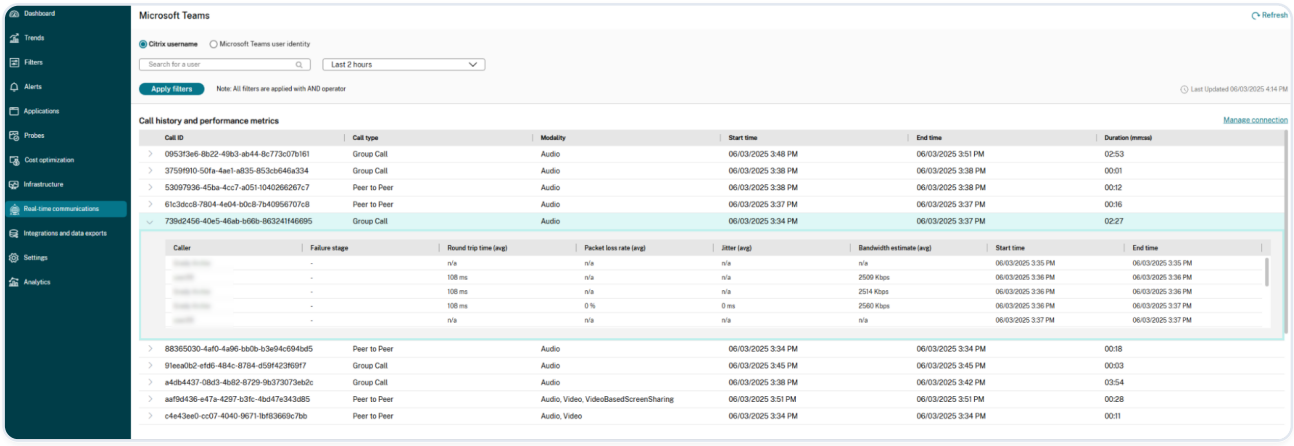
- Descrição: A inicialização da continuidade do serviço falhou devido ao bloqueio e/ou revogação do lease.
- Ação Recomendada: Entre em contato com o administrador do Citrix Cloud com os detalhes do erro. Para obter mais informações, consulte a documentação de continuidade do serviço.
  - Se o problema persistir, entre em contato com o suporte da Citrix.

Painel de comunicações em tempo real

Microsoft Teams

O painel do Microsoft Teams no Citrix Director oferece visibilidade das chamadas do Microsoft Teams entre os usuários, juntamente com detalhes sobre os participantes e métricas que indicam o desempenho da chamada. O painel oferece a capacidade de:

- Avaliar o resumo de uso do Microsoft Teams
- Filtrar e ver detalhes das chamadas do Microsoft Teams para a duração selecionada
- Avaliar chamadas individuais usando métricas de desempenho



Pré-requisitos

Adicione a Interface de Programação de Aplicativos (API) do Microsoft Graph à lista de permissões no Citrix Director:

- Para que o Director acesse os registros de chamadas, certifique-se de que o acesso à internet de saída esteja disponível em todas as máquinas onde o Director está instalado. Especificamente, certifique-se de que a URL `https://graph.microsoft.com` esteja acessível
- Se você usa um servidor proxy, certifique-se de que a URL da API do Microsoft Graph: `https://graph.microsoft.com` esteja acessível.

Introdução

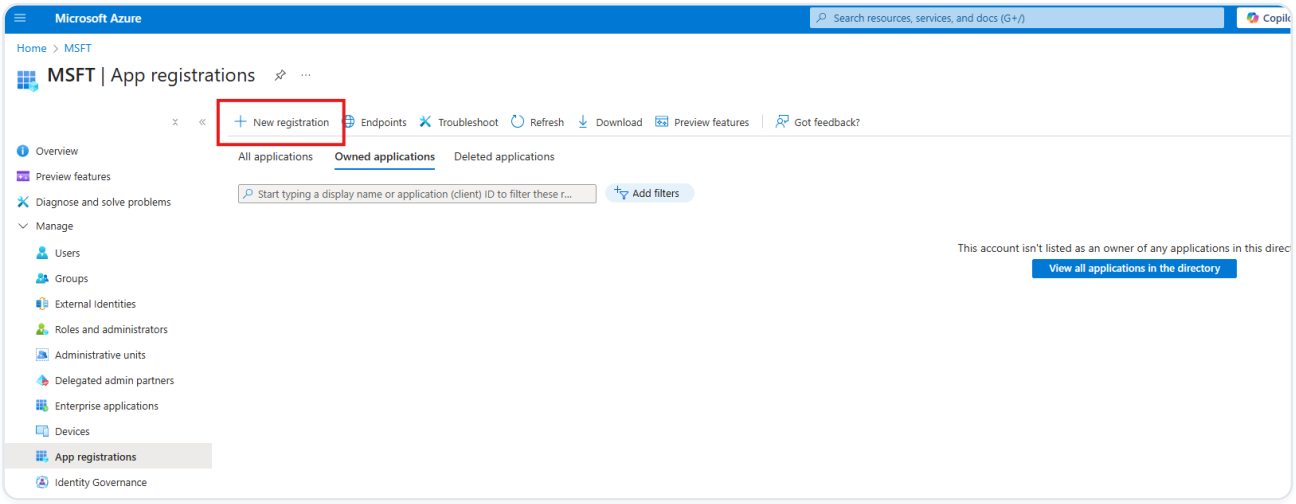
Conexão com a API do Microsoft Graph

Os detalhes das chamadas da Microsoft são obtidos da API do Microsoft Graph. Para que o Citrix Director acesse a API, um aplicativo precisa ser criado no Microsoft Entra ID com as permissões necessárias. A URL da API do Graph também precisa ser adicionada à lista de permissões no Director.

Execute as seguintes etapas para concluir a conexão:

Etapa 1: Registro de aplicativo no Microsoft Entra ID

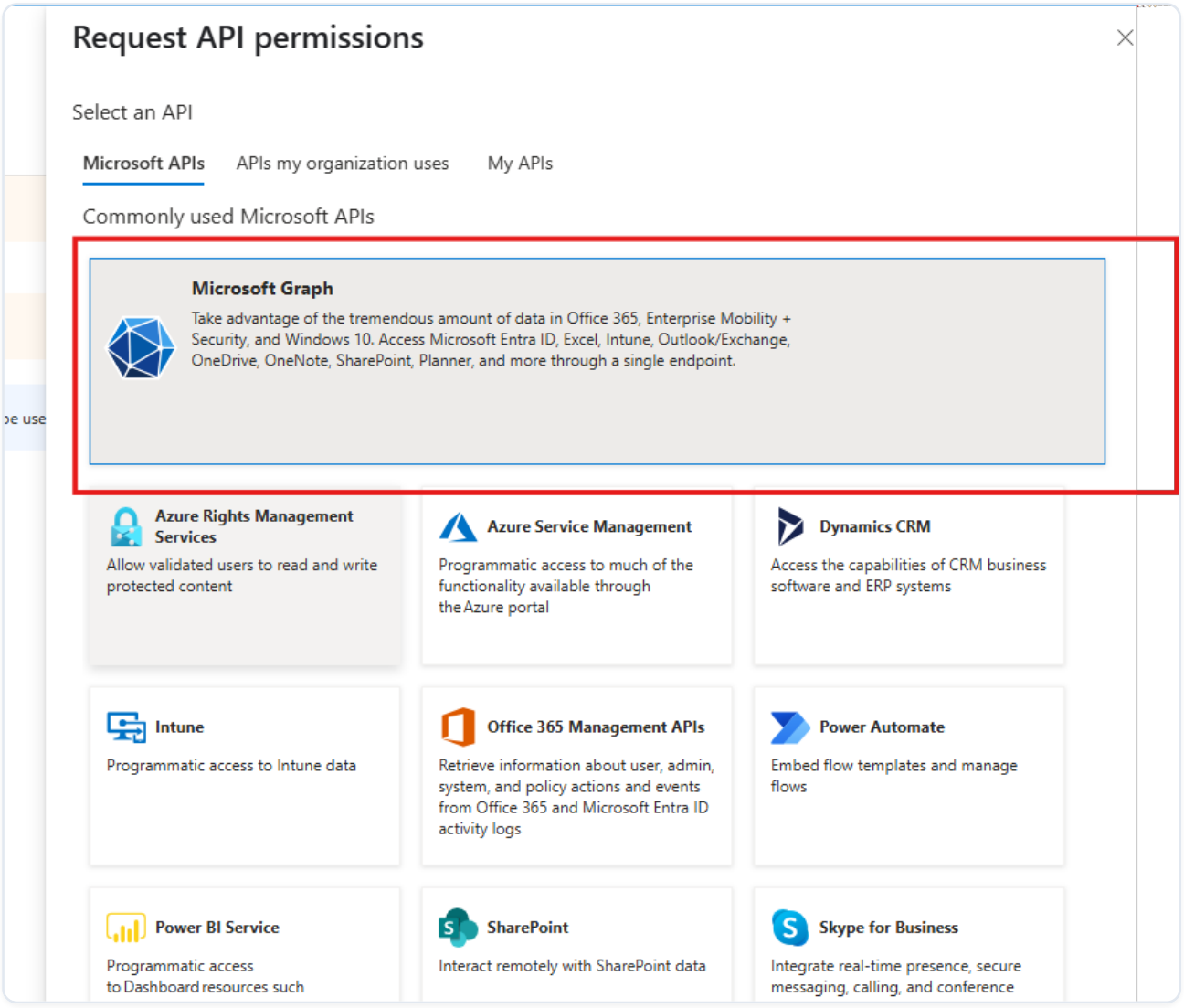
1. navegar para **Registros de aplicativo -> Novo registro** no Microsoft Entra ID.



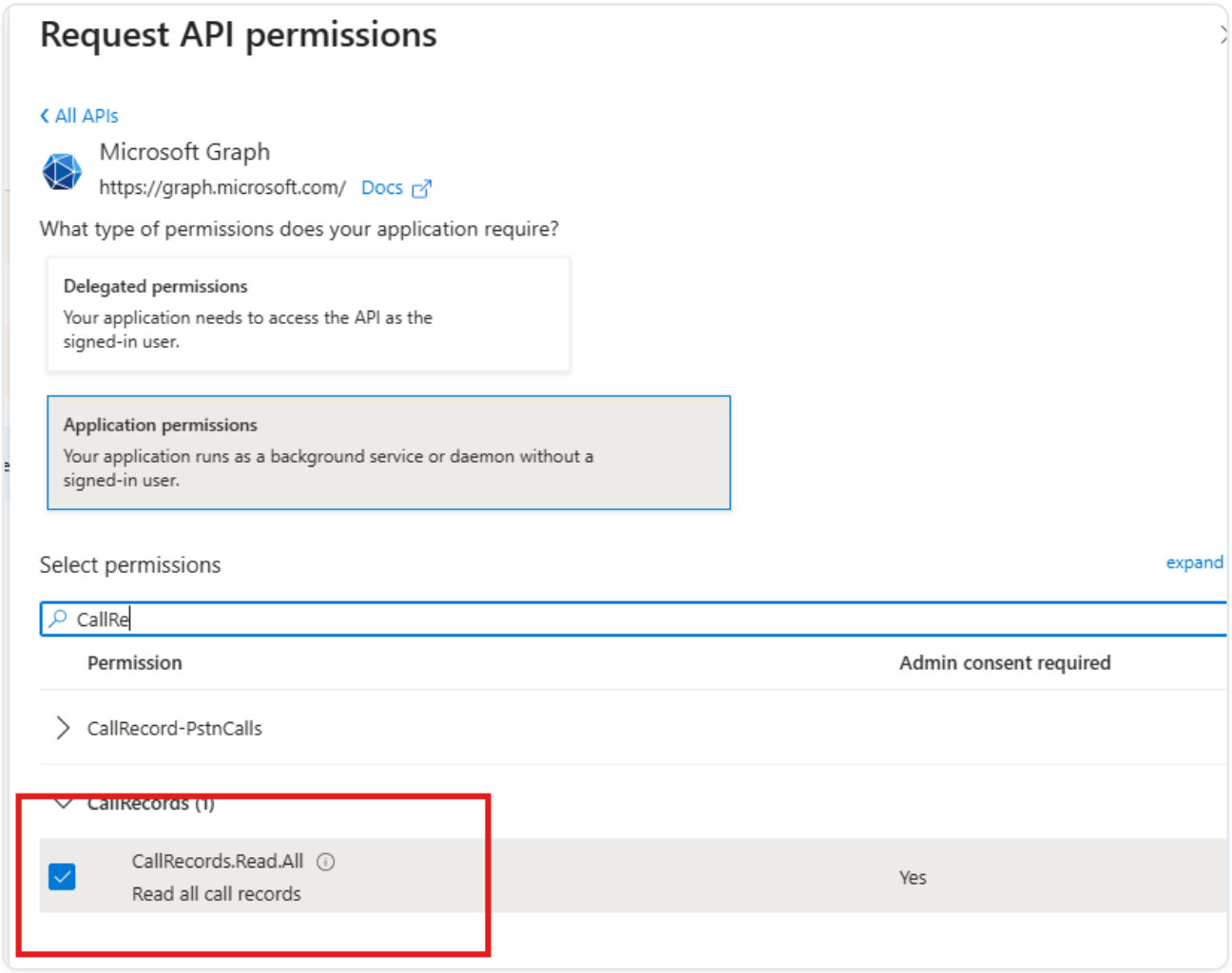
1. Execute as etapas necessárias para o registro do aplicativo.
2. Após o registro, copie o ID do Cliente e o ID do Locatário do aplicativo.

ETAPA 2: ADICIONANDO PERMISSÕES DO MICROSOFT GRAPH NO MICROSOFT ENTRA ID

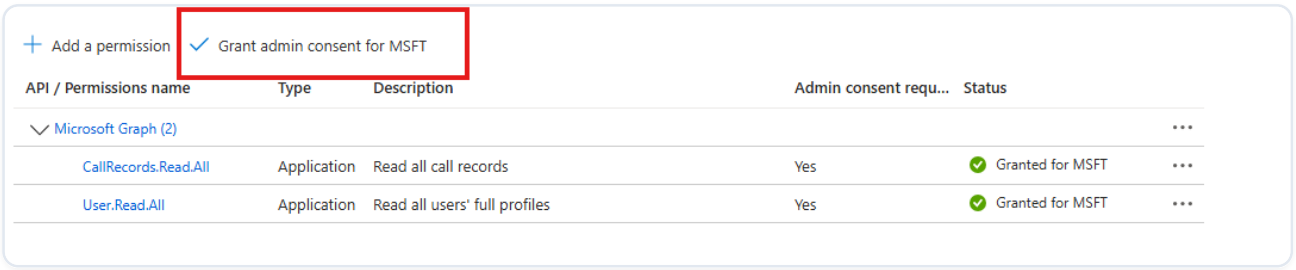
1. navegar para **Permissões de API -> Adicionar uma permissão.**
2. Selecione **Microsoft Graph** e depois **Permissões de aplicativo.**



1. Adicione permissões para **CallRecords.Read.All** e **User.Read.All**

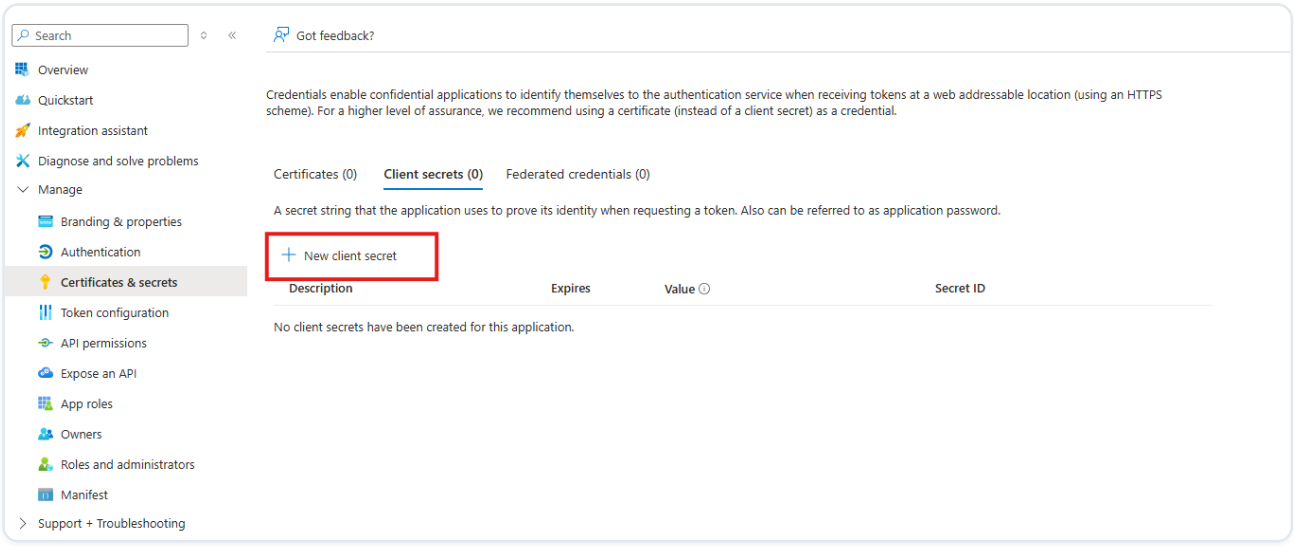


1. Clique em Grant admin consent for MSFT. Esta ação requer um administrador global do Entra ID.



Etapa 3: Criando um Segredo do Cliente

1. No Microsoft Entra ID, navegar para **Certificados e segredos > Novo segredo do cliente**. Você também pode reutilizar um segredo existente.

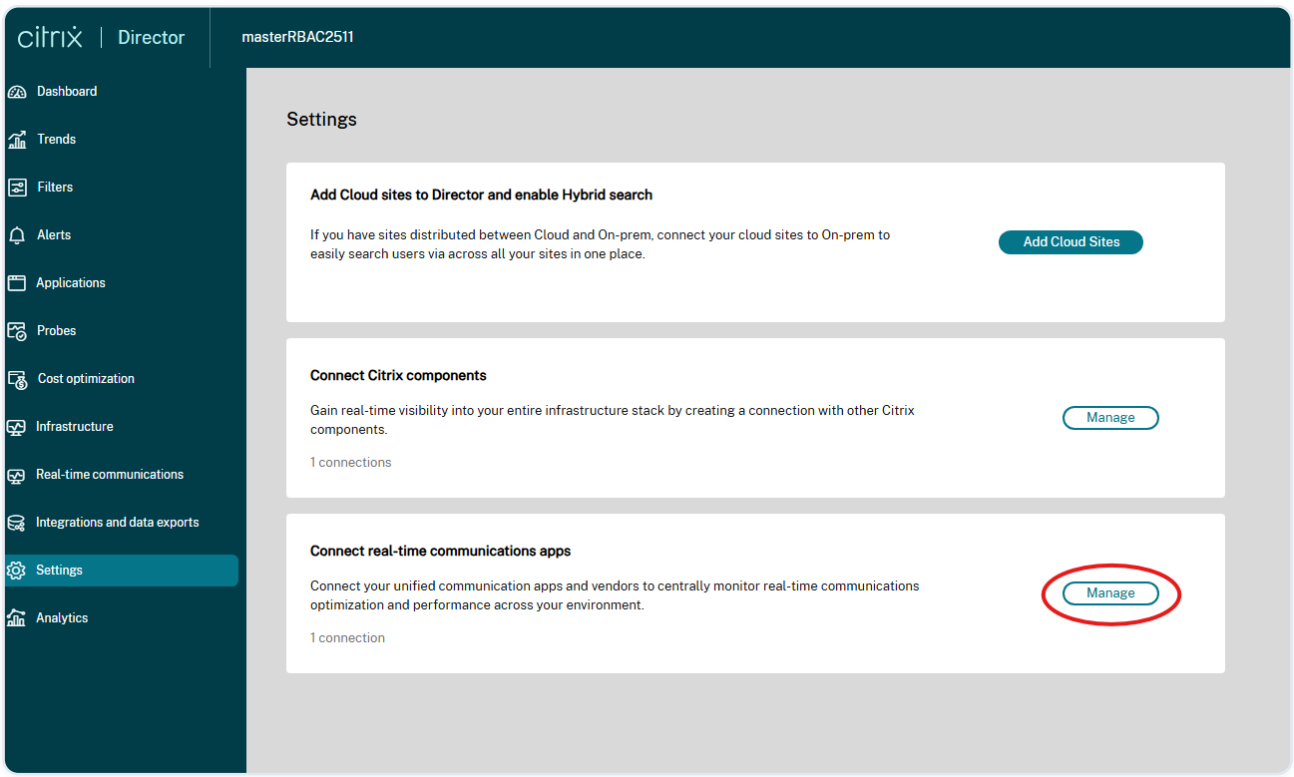


1. Forneça um nome e uma data de expiração para o segredo. Certifique-se de que o segredo seja renovado antes da expiração para manter a conexão.
2. Copie o segredo do cliente para usar na interface do usuário do Director.

Para obter mais informações, consulte a documentação oficial do Azure se você enfrentar algum problema.

Etapa 4: Concluir a Conexão no Director

1. No Director, navegar para **Settings -> Connect real-time communications apps**.



1. Clique em **Create connection** e insira o ID do Aplicativo, ID do Diretório e Segredo do Cliente copiados do registro do aplicativo.

Create a connection

Choose the application type you want to establish a connection with.

Application type

Microsoft Teams

To connect to Microsoft Teams, register a client application in Microsoft Entra ID and ensure it meets the prerequisites for a successful connection. Then, enter the required credentials. Learn more

Registered application

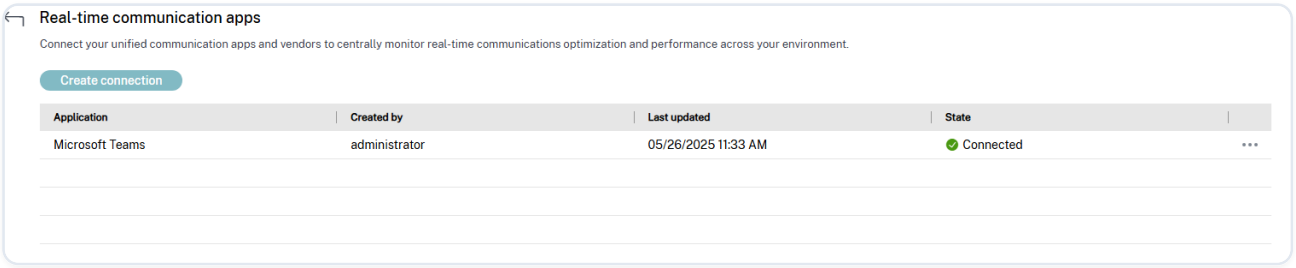
Application (client) ID

Directory (tenant) ID

Client secret

Create Cancel

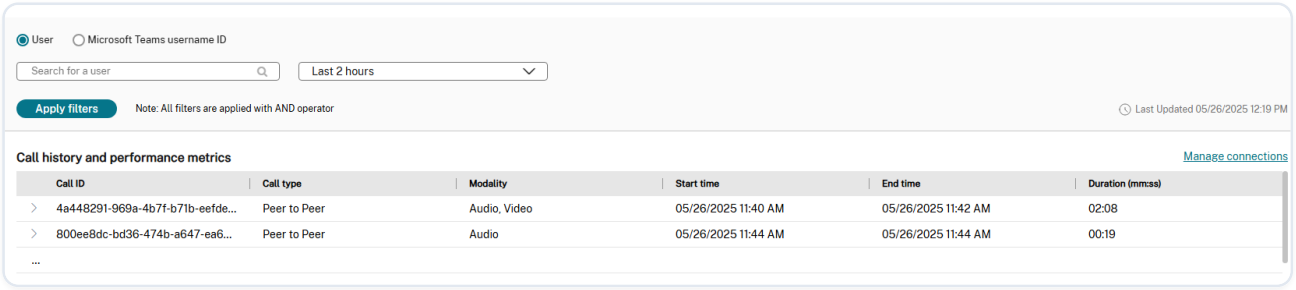
A conexão é estabelecida com sucesso se credenciais válidas e permissões para buscar detalhes da chamada estiverem disponíveis.



1. Você pode **Editar** e **Excluir** a conexão clicando nas reticências no final da linha.

Painel do Microsoft Teams

navegar para a guia **Real time Communications** na interface do usuário do Director. O painel do Microsoft Teams é preenchido com os dados coletados da conexão do Microsoft Graph estabelecida. Os detalhes da chamada ficam disponíveis aproximadamente 15 minutos após o término da chamada.

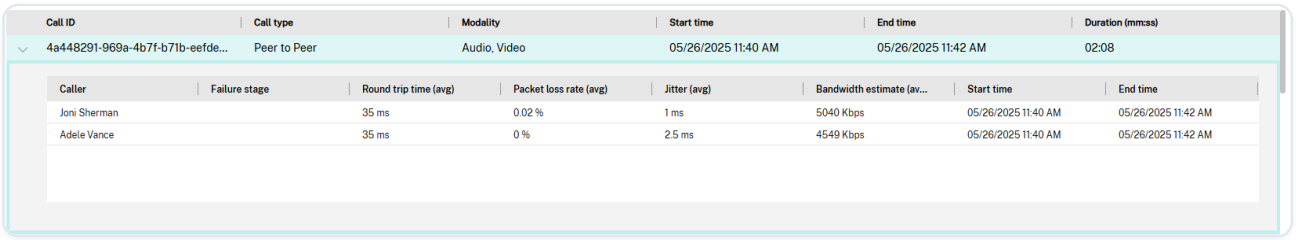


A exibição da tabela fornece os seguintes detalhes em todas as chamadas.

NOME DA COLUNA	DESCRIÇÃO
ID da Chamada	Um identificador exclusivo para cada chamada.
Tipo de chamada	Indica se a chamada é ponto a ponto ou uma chamada em grupo.
Modalidade	Indica quais modos são usados durante a chamada, como áudio, vídeo ou compartilhamento de tela.
Hora de início	A data e a hora em que a chamada começou.
Hora de término	A data e a hora em que a chamada terminou.

NOME DA COLUNA	DESCRIÇÃO
Duração (mm: ss)	Duração da chamada em minutos e segundos.

Clique nas chamadas individuais na tabela para visualizar os detalhes de falha e desempenho por usuário.



Em uma chamada em grupo, quando um usuário se desconecta e se reconecta, isso é considerado uma sessão separada. Essa consideração ajuda a identificar problemas específicos, como maior latência ao se conectar a uma rede específica.

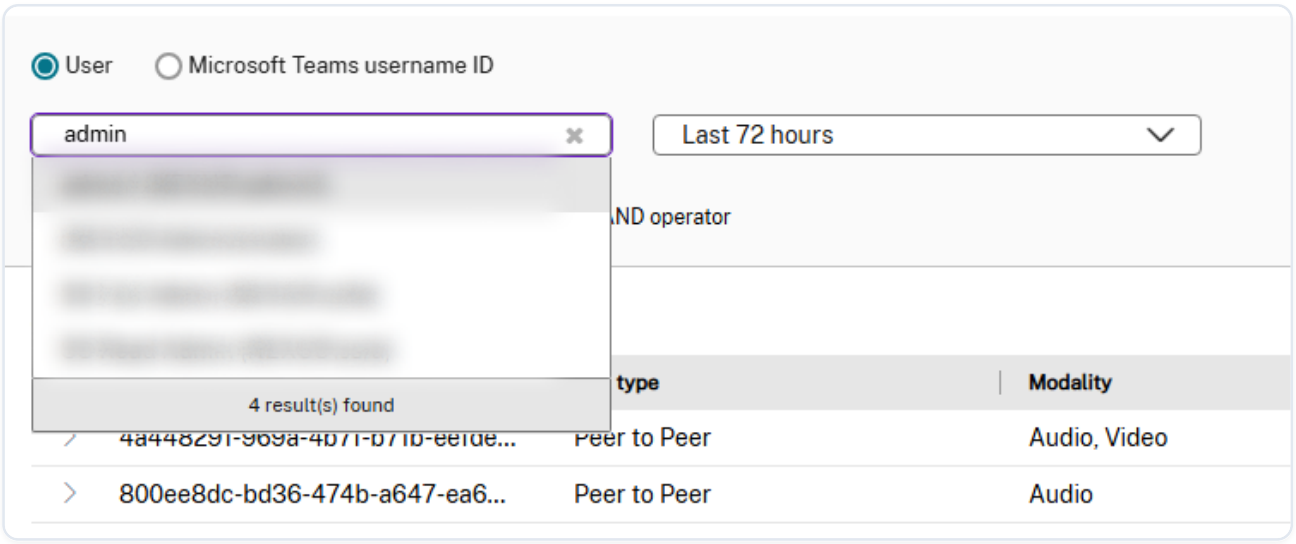
Cada linha na tabela de detalhes da chamada contém as seguintes informações:

NOME DA COLUNA	DESCRIÇÃO
Hora de início	A data e hora em que a chamada ou o segmento do participante começou.
Tempo de ida e volta (médio)	Tempo médio de ida e volta para pacotes de dados.
Taxa de perda de pacotes (médio)	Porcentagem média de pacotes perdidos durante a chamada.
Jitter (médio)	Variação média no atraso dos pacotes recebidos.
Estágio da falha	Indica o estágio em que ocorreu uma falha na chamada, como durante a configuração ou no meio da chamada.
Hora de término	Data e hora em que a chamada ou o segmento do participante terminou.
Chamador	Nome do participante na chamada.

NOME DA COLUNA	DESCRIÇÃO
Estimativa de largura de banda (média)	Largura de banda média estimada usada durante a chamada.

Você pode filtrar usuários de duas maneiras: por nome de usuário Citrix ou por nome de usuário do Microsoft Teams. Você pode alternar entre essas opções usando os botões de rádio na parte superior da página.

- **Nome de usuário Citrix:** Ao começar a digitar um nome de usuário, o sistema sugere usuários correspondentes. Você pode então selecionar a conta específica para visualizar os detalhes.
- **Nome de usuário do Microsoft Teams:** Use esta opção se o e-mail ou o Nome Principal do Usuário (UPN) associado à conta do Microsoft Teams for diferente do ID da conta Citrix. Ao usar este método, você deve inserir o endereço de e-mail completo e válido.



Painel de monitoramento de continuidade de serviço

Visão geral

O Painel de Monitoramento de Continuidade de Serviço fornece aos administradores visibilidade centralizada e imediata sobre lacunas de configuração e vulnerabilidades de usuários finais que poderiam impedir o funcionamento da Continuidade de Serviço durante uma interrupção na nuvem. Ao monitorar a prontidão, os administradores podem usar os dados de prontidão para detecção precoce, tomar ações corretivas para garantir que os usuários mantenham o acesso aos seus aplicativos e desktops, reduzindo, em última análise, o impacto comercial das interrupções.

O que é uma instância e como os dados são coletados dela?

Uma instância representa uma forma única de um usuário acessar o Citrix Workspace™, com base no usuário, no dispositivo e na forma como ele faz login. Por exemplo, se um usuário faz login em um dispositivo usando Chrome, Edge e o aplicativo Citrix Workspace, cada método de acesso é rastreado como uma instância separada. Cada instância envia um evento aproximadamente uma vez a cada 24 horas.

Como a prontidão é calculada

Para que uma instância seja considerada pronta, ela deve satisfazer as seguintes condições. Se alguma delas não for atendida, a instância é considerada "Não pronta".

Para inicialização de aplicativo nativo

- A continuidade do serviço está habilitada
- Pelo menos um recurso alugável (aplicativo ou desktop) está disponível
- Pelo menos um lease de conexão válido existe
- Nenhum lease de conexão expirado está presente

Para inicialização híbrida (login pela web, inicialização de sessão via aplicativo CWA)

- A continuidade do serviço está habilitada
- A extensão da web Citrix está instalada
- Pelo menos um recurso alugável (aplicativo ou desktop) está disponível
- Pelo menos um lease de conexão válido existe
- Nenhum lease de conexão expirado está presente

Requisitos de versão

Os dados de prontidão da continuidade do serviço estão disponíveis com certas versões do aplicativo Citrix Workspace e superiores.

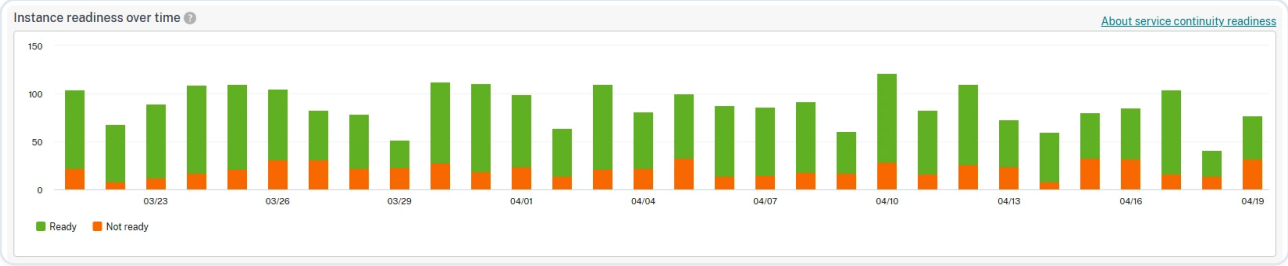
PLATAFORMA	VERSÃO MÍNIMA SUPORTADA
Híbrido (login pela web, inicialização da sessão via aplicativo CWA)	Atualizado automaticamente
CWA Windows	2511

PLATAFORMA	VERSÃO MÍNIMA SUPORTADA
CWA Mac	2603
CWA Linux	2503
CWA Android	2603
CWA iOS	2603

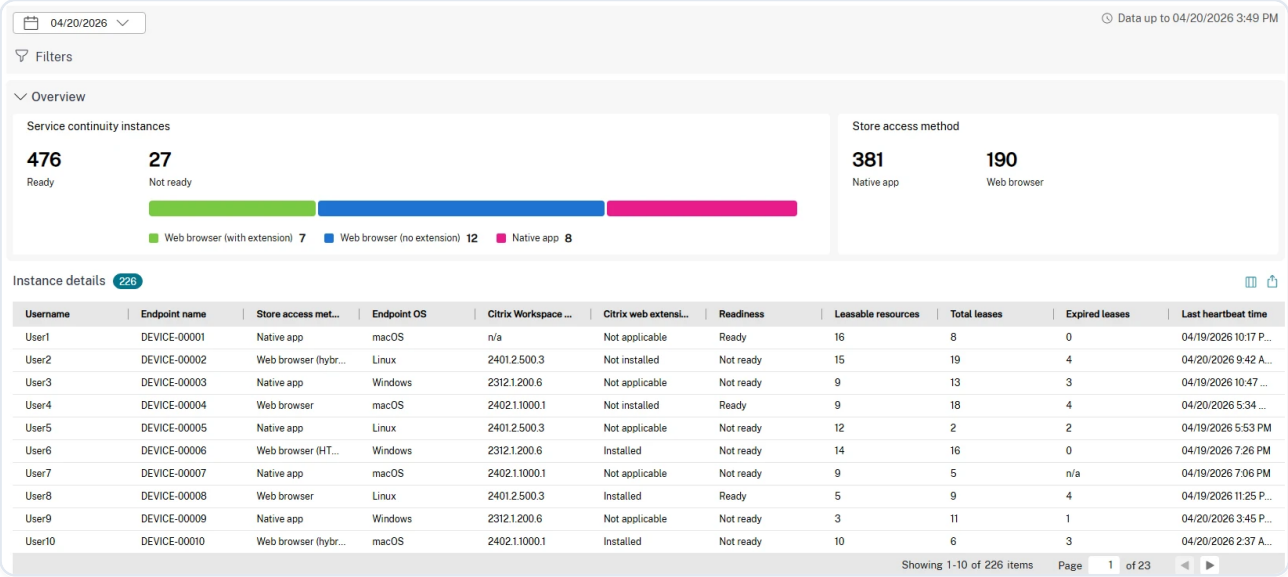
Recursos do painel

Gráfico de prontidão da instância ao longo do tempo

Um gráfico de barras de prontidão de 30 dias que representa a contagem de prontidão em cada dia. A seção verde representa as instâncias "Prontas", enquanto a seção laranja representa as instâncias "Não prontas".



Painel de visão geral diária e gráficos de instância



Estas duas seções representam os dados correspondentes a um único dia. Por padrão, o dia atual é selecionado. Os usuários podem ver os dados diários dos últimos 7 dias e podem analisar esses dados usando diferentes filtros. Os dados diários são limitados a 7 dias porque os registros de

instâncias individuais são retidos por esse período, enquanto os resumos diários por trás do gráfico de 30 dias são retidos por 30 dias.

O dia atual ainda está em andamento. Como cada instância relata aproximadamente uma vez a cada 24 horas, as contagens de hoje se acumulam ao longo do dia e são menores do que as de um dia completo. Selecione um dia anterior para uma visualização completa.

Painel de visão geral

O painel de visão geral contém as seguintes subseções:

1. **Instâncias de continuidade do serviço**

   Ele mostra a contagem de instâncias Prontas e Não prontas. Um gráfico é exibido abaixo da seção "Não prontas", mostrando uma divisão por plataforma das instâncias não prontas.

2. **Método de acesso à Store**

   Esta seção representa a divisão diária do método de acesso à store do usuário. O aplicativo nativo representa logins do aplicativo Citrix Workspace em plataformas como Windows, Linux e Android, enquanto o navegador da Web mostra logins da store por meio de um navegador ou plataformas HTML5.

Detalhes da instância

Os detalhes da instância consistem em todos os eventos de prontidão recebidos ao longo do dia selecionado. Cada linha representa uma única instância. A tabela também pode ser exportada como um arquivo CSV.

Filtros

Os dados podem ser filtrados usando o filtro de data e filtros baseados em campos de dados. Os seguintes campos de dados são suportados:

- Versão do aplicativo Citrix Workspace
- SO do endpoint
- Prontidão
- Método de acesso à Store

Campos da tabela

As colunas são agrupadas em Usuário, Endpoint e Continuidade do serviço. Use **Gerenciar colunas** para adicionar ou remover as opcionais.

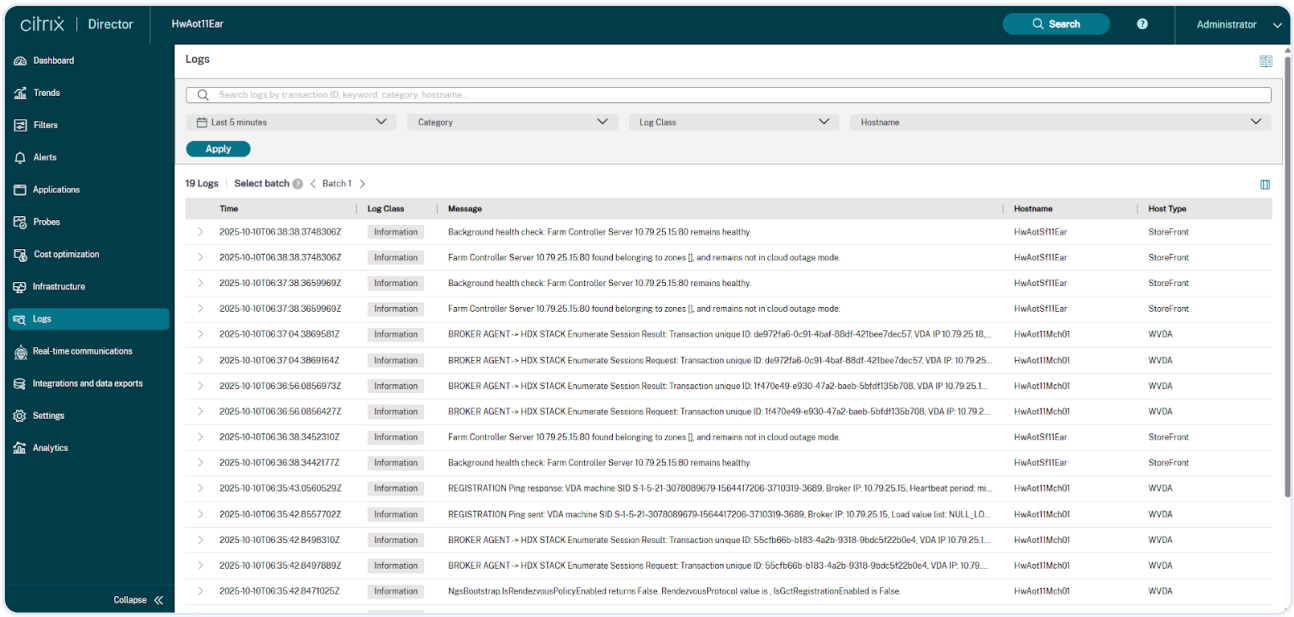
CATEGORIA	CAMPO	INFORMAÇÕES	VISÍVEL POR PADRÃO
Usuário	Nome de usuário	O nome de usuário do usuário	Sim
Ponto de extremidade	Nome do ponto de extremidade	O nome do host do ponto de extremidade do usuário	Sim
Ponto de extremidade	Método de acesso à loja	Como o usuário está acessando a loja - aplicativo CWA ou via navegador	Sim
Ponto de extremidade	SO do Endpoint	Plataforma do SO do Endpoint (Windows, macOS, Android e assim por diante)	Sim
Endpoint	Versão do aplicativo Citrix Workspace	O número da versão do aplicativo nativo instalado	Sim
Endpoint	Extensão da web Citrix	Indica se o usuário instalou a extensão da web Citrix. É "não aplicável" para um lançamento nativo puro	Sim
Continuidade do serviço	Prontidão	Prontidão com base na fórmula explicada acima (Pronto/Não pronto)	Sim
Continuidade do serviço	Recursos arrendáveis	A contagem de recursos arrendáveis (aplicativos e desktops) aos quais o usuário tem acesso. Estes	Sim

CATEGORIA	CAMPO	INFORMAÇÕES	VISÍVEL POR PADRÃO
		podem ser iniciados em um cenário de interrupção parcial	
Continuidade do serviço	Total de arrendamentos	Contagem total de arrendamentos no dispositivo do usuário quando a sincronização ocorreu	Sim
Continuidade do serviço	Arrendamentos expirados	Contagem de arrendamentos expirados no dispositivo do usuário quando a sincronização ocorreu	Sim
Continuidade do serviço	Última sincronização de arrendamento	A última vez que o dispositivo do usuário sincronizou os arquivos de arrendamento. Por padrão, a sincronização de arrendamento ocorre a cada 6 horas	Não
Continuidade do serviço	Hora do último heartbeat	O carimbo de data/hora em que os dados do usuário foram sincronizados com o painel. Cada instância envia um heartbeat com todas as informações relevantes aproximadamente	Sim

CATEGORIA	CAMPO	INFORMAÇÕES	VISÍVEL POR PADRÃO
		uma vez a cada 24 horas.	

Logs

A nova Visualização de Logs no Citrix Director/Monitor foi projetada para apresentar o Rastreamento Sempre Ativo (AOT) para aprimorar significativamente a capacidade de um administrador de diagnosticar e resolver problemas de clientes em ambientes Citrix Virtual Apps and Desktops (CVAD). Ao integrar-se com seu Servidor de Logs Centralizado, este recurso fornece uma visualização unificada e pesquisável dos logs AOT em vários componentes principais, incluindo Virtual Delivery Agents, Delivery Controllers, StoreFront e outros componentes Citrix. Este acesso centralizado simplifica a solução de problemas, permitindo a recuperação e análise rápidas de logs a partir de um único console.



Saiba mais sobre a arquitetura e os benefícios do Rastreamento Sempre Ativo (AOT) na documentação do produto.

Pré-requisitos e Configuração

Para usar efetivamente a visualização de “Logs” no Director, seu ambiente precisa ser configurado corretamente e atender aos pré-requisitos necessários.

- **Requisito de Versão do CVAD**: Você deve estar executando o CVAD 2507 CU1 ou CVAD 2511 (ou uma versão posterior).

- Servidor de Logs Centralizado: Sua Localização de Recurso gerenciada pelo cliente deve hospedar um Servidor de Logs Centralizado. Saiba mais sobre Instalar e Configurar seu Servidor de Logs
- Quando o servidor de logs é configurado no modo HTTPS (por exemplo, `https://<LogServerFQDN>:port`), é essencial instalar e confiar no certificado necessário nas máquinas Director e DDC. Este certificado deve ser gerenciado pela conta do computador em cada máquina.
- **Requisito do Cloud Connector**: O Cloud Monitor recupera logs AOT através do **serviço Monitor Connector em execução em um Cloud Connector Windows compatível** na Localização de Recurso. Um Cloud Connector Windows compatível também deve estar presente na mesma Localização de Recurso. O Cloud Connector deve estar executando a versão **6.141.0.13739** (ou **4.420.0.13739**) ou posterior.

Introdução

Uma vez que as configurações de pré-requisito estejam concluídas, a nova guia Logs na interface do usuário do Director fornecerá visibilidade unificada aos seus logs AOT centralizados.

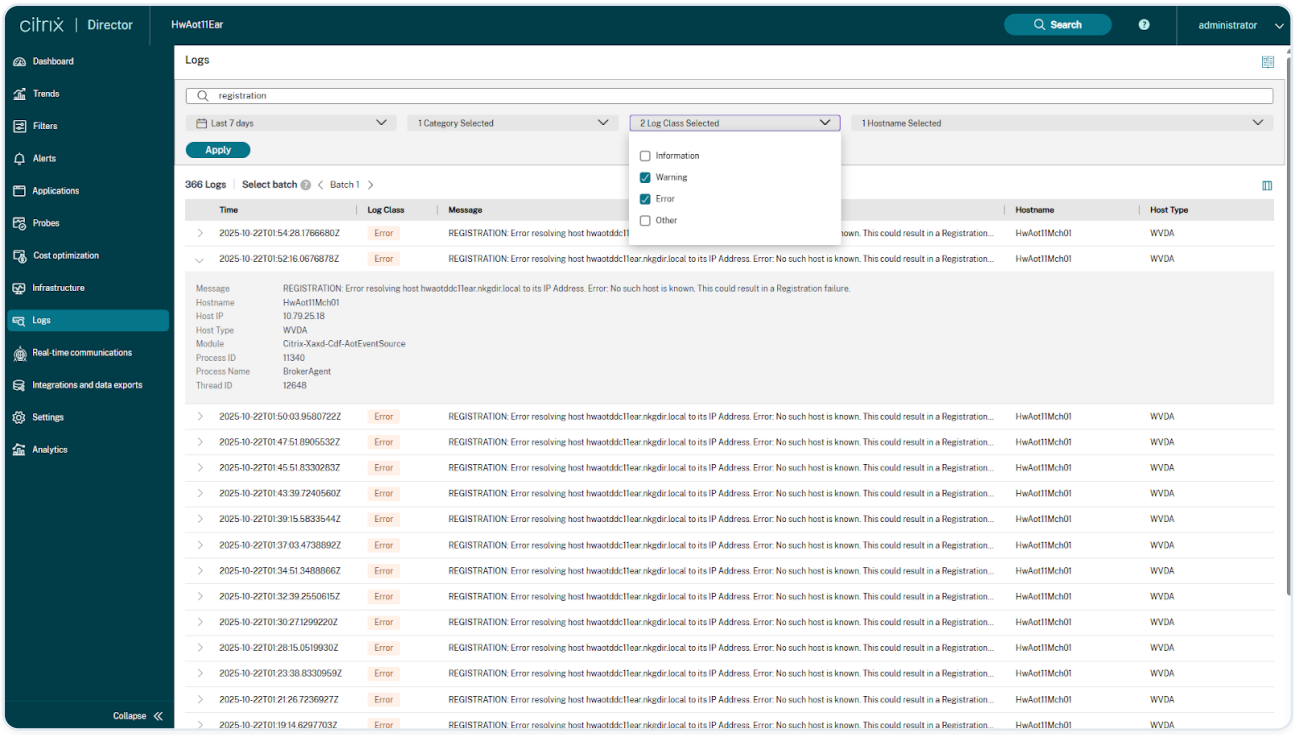
Acessando a Visualização de Logs

A Visualização de Logs pode ser acessada diretamente como uma guia dedicada dentro do Director, ou navegada contextualmente a partir de outras áreas-chave de solução de problemas:

- **Guia “Logs” Dedicada**: Acesse a nova página "Logs" diretamente na interface do Director/Monitor usando o painel de navegação.
- **Gerenciador de Atividades**: Clique em uma opção para visualizar logs relacionados para a máquina que hospeda a sessão.
- **Filtros de Máquina**: Clique em uma opção para visualizar logs relacionados com um nome de Máquina preenchido previamente.

Usando a Visualização de Logs

A Visualização de Logs foi projetada para uma pesquisa de log flexível e poderosa, permitindo que os administradores identifiquem rapidamente eventos relevantes.



A interface de pesquisa principal inclui:

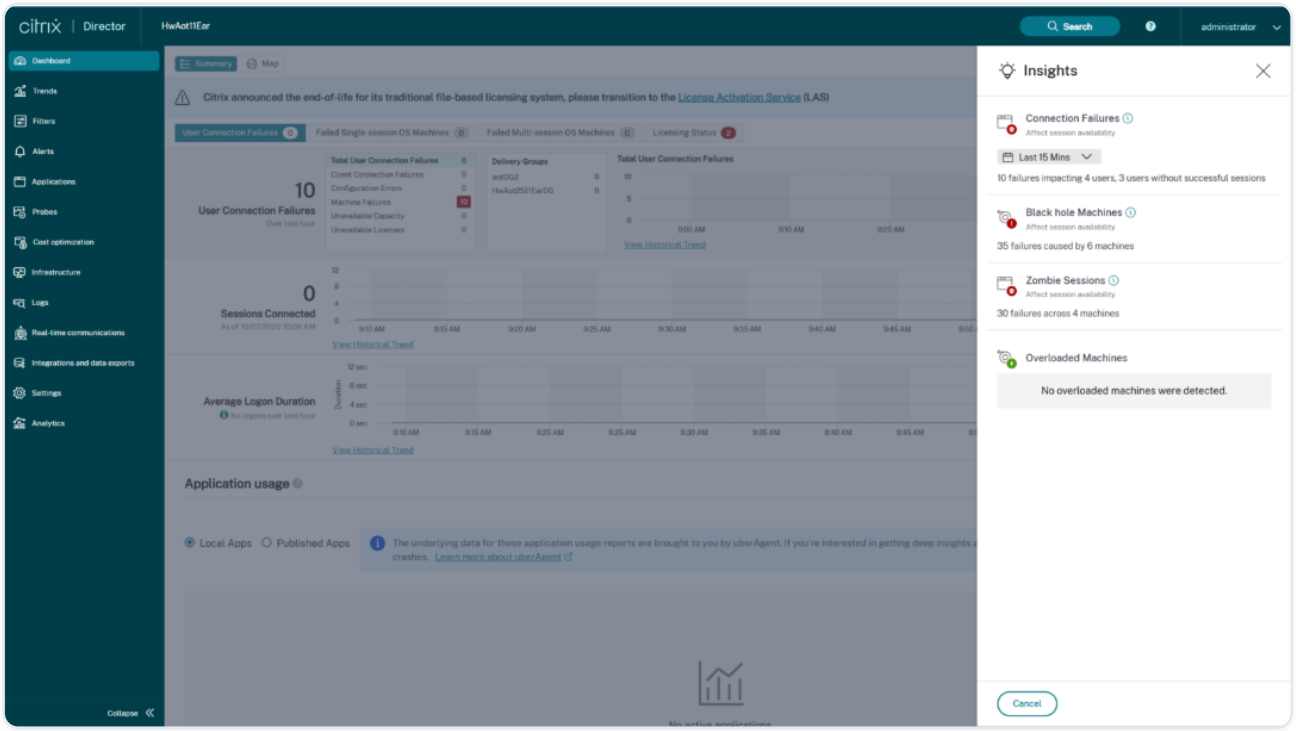
- **Barra de Pesquisa**: Uma caixa de texto poderosa que permite pesquisar por qualquer palavra-chave. Termos de pesquisa comuns incluem ID da Transação, ID da Sessão, Nome de Usuário ou mensagens de erro específicas.
- **Seletores de Filtro**: Use os seguintes filtros suspensos para restringir o escopo da sua pesquisa:
- **Intervalo de Tempo**: Filtre logs por um intervalo de tempo específico.
- **Categoria**: Filtre por categoria de log.
- **Classe de Log**: Filtre pela classe da mensagem de log (por exemplo, AOT_INFO).
- **Nome da máquina**: Filtre logs originados de um nome de máquina específico.

Os resultados da pesquisa são apresentados em um formato de tabela abrangente com atributos chave como Hora, Mensagem, Nome do Host, Nível, Módulo, ID do Processo e muito mais. Você pode expandir entradas de log individuais para visualizar detalhes completos. O Director oferece suporte à configuração e visualização de colunas personalizadas relevantes para seus dados de log. Além disso, os resultados são paginados para facilitar a visualização e navegação em grandes conjuntos de dados.

Ao fornecer acesso imediato e sensível ao contexto a todos os logs AOT, este recurso visa reduzir o tempo gasto na troca entre ferramentas e na correlação manual de logs, levando a uma resolução de problemas mais rápida.

Insights

O painel Insights fornece informações sobre falhas de sessão ou lentidão em seu ambiente. Aprofundar-se em métricas específicas com esses insights ajuda a solucionar e resolver falhas de sessão ou lentidão mais rapidamente. Os Insights de Falha ajudam especificamente os administradores a melhorar a disponibilidade da sessão, que é um fator importante que determina a experiência do usuário. Esses insights são projetados para auxiliar no monitoramento proativo da experiência do usuário. Assim, os Insights são exibidos para as falhas atuais no sistema (atualizados a cada 15 minutos).



Clicar no ícone de insights no Painel exibe o painel de insights com detalhes sobre os insights e opções para detalhar a visualização de Máquinas ou Conexões. O administrador também pode navegar para a configuração de alertas a partir do painel.

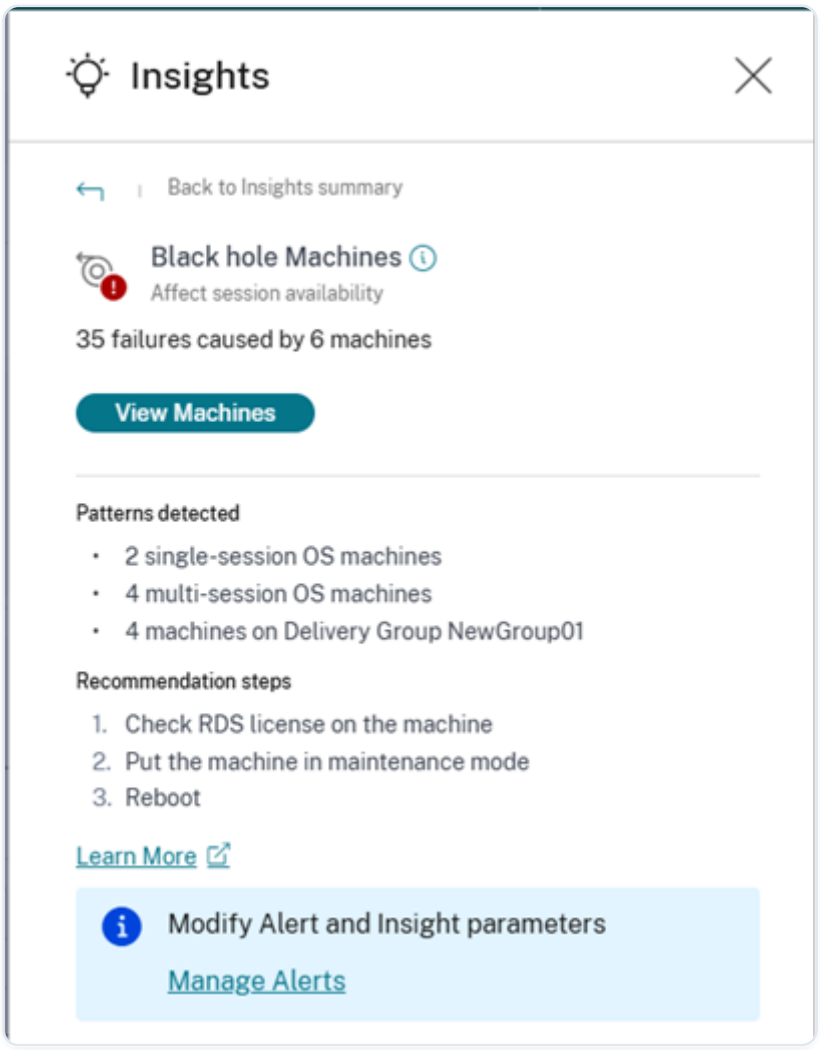
Máquinas Blackhole, Sessões Zombie, Máquinas Sobrecargadas e Insights de falha de sessão estão disponíveis neste painel. Cada insight, ao ser expandido, exibe um link para as sessões com falha ou para as máquinas que as hospedam. Isso leva à visualização de Filtros contendo as máquinas ou sessões com falha. Um detalhamento adicional é possível a partir daqui ao clicar em uma máquina ou sessão específica para ver as métricas detalhadas.

A visualização expandida para cada insight mostra os principais padrões de falha detectados em relação ao site, Grupo de Entrega, máquinas de sessão de SO único ou multi-SO. Esses padrões visam ajudar os administradores a identificar se há uma coorte específica de usuários enfrentando o problema. Nos casos em que o sistema não consegue destacar nenhum padrão devido a uma

coorte distribuída, é recomendado detalhar para autoanálise. Além disso, são mostradas as ações recomendadas para solucionar e resolver os problemas.

Máquinas black hole

Algumas máquinas em seu ambiente, embora registradas e aparentemente saudáveis, podem não atender às sessões intermediadas a elas, resultando em falhas. Máquinas que falharam em atender quatro ou mais solicitações de sessão consecutivas são denominadas máquinas black hole. As razões para essas falhas estão relacionadas a vários fatores que podem afetar a máquina, como licenças RDS insuficientes, problemas intermitentes de rede ou carga instantânea na máquina. Essas falhas não incluem falhas devido à capacidade ou disponibilidade de licença. A presença de máquinas black hole no ambiente aumenta as falhas de sessão, resultando em baixa disponibilidade de sessão. Os insights de máquinas black hole mostram o número de máquinas black hole identificadas em seu ambiente.



Ações recomendadas para máquinas black hole:

- Verificar licença RDS na máquina

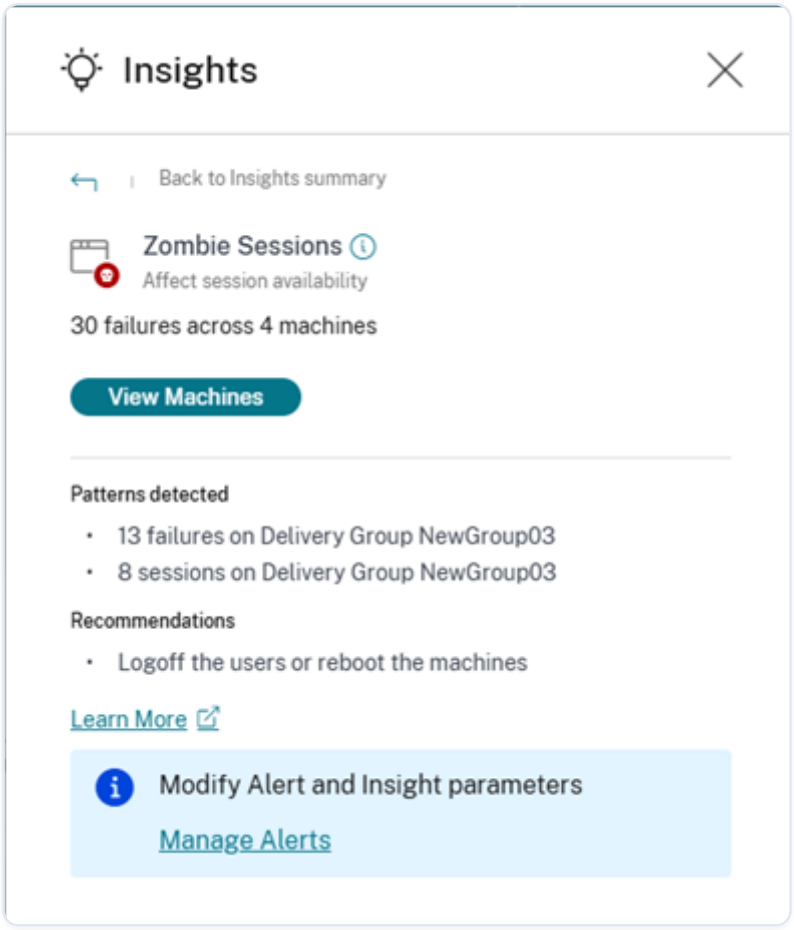
- Colocar a máquina em modo de manutenção
- Reiniciar

A seção Padrões Detectados mostra os principais padrões observados em máquinas black hole em relação aos seguintes critérios:

- Número de máquinas black hole executando SO de sessão única ou multi-sessão
- Grupo de Entrega com o maior número de máquinas impactadas

Sessões Zumbis

O subpainel Sessões Zumbis mostra informações sobre falhas de sessão que ocorreram devido a sessões zumbis no ambiente. Uma sessão zumbi é uma sessão abandonada em uma máquina de SO de sessão única, resultando na falha de novos inícios de sessão na máquina. As tentativas de iniciar sessões nesta máquina falham com um erro de “Capacidade Indisponível”. Todas as futuras tentativas de iniciar sessões falham até que a sessão abandonada seja encerrada. Os insights de sessão zumbi visam ajudar a identificar essas máquinas com sessões abandonadas e a mitigar proativamente essas falhas.



Ações recomendadas para Sessões Zumbis:

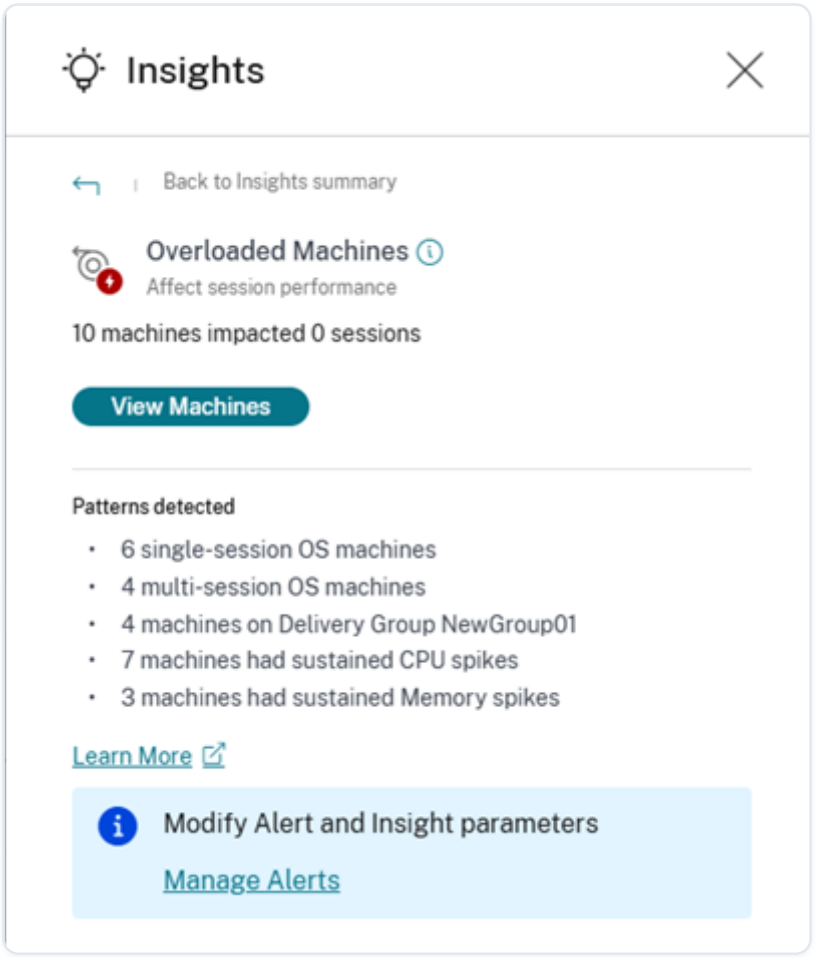
- Você pode desconectar os usuários das sessões Zumbis usando o Monitor para sites Citrix DaaS.
- Você pode reiniciar as máquinas que contêm sessões Zumbis.

A seção Padrões detectados mostra os principais padrões observados nas sessões Zumbis em relação aos seguintes critérios:

- Grupo de Entrega com o maior número de máquinas impactadas
- Grupo de Entrega com o maior número de sessões impactadas

Máquinas Sobrecargadas

O Insight de Máquinas Sobrecargadas oferece visibilidade sobre recursos sobrecarregados que causam uma experiência ruim. Máquinas que experimentaram picos sustentados de CPU, ou alto uso de memória, ou ambos, que duraram 5 minutos ou mais, e que podem resultar em uma experiência de usuário ruim, são consideradas sobrecarregadas.



A seção Padrões Detectados mostra os principais padrões observados em máquinas sobrecarregadas em relação aos seguintes critérios:

- Número de máquinas sobrecarregadas executando SO de sessão única ou multi-sessão

- Grupo de Entrega com o maior número de máquinas impactadas
- Número de máquinas sobrecarregadas com picos sustentados de memória ou CPU

Falhas de conexão

O insight de Falhas de Conexão lista o número de falhas de sessão devido a problemas desde o endpoint (onde o usuário inicia a sessão) até a máquina (onde a sessão é intermediada). Essas falhas podem ocorrer devido a uma variedade de razões, desde configurações incorretas de firewall, problemas de comunicação de rede ou indisponibilidade da máquina.

Insights

Back to Insights summary

Connection Failures

Affect session availability

Last 24 Hours

14 failures impacting 5 users, 4 users without successful sessions

All failures | No successful connections

Patterns detected

Client Connection Failures

- 9 (75%) errors in top failure reason ConnectionTimeout
- 8 failures are on Delivery Group MultiDG-0806

Machine Failures

- 1 (50%) errors in top failure reason MachineNotFunctional
- 2 failures are on Delivery Group MultiDG-0806
- 2 errors from 1 machines which are in unregistered or powered off state

View all connection failures

Recommended action

- Check the firewall settings on the machine and gateway
- Check network connectivity between the components
- Ensure the machine is powered on, and in registered states

As duas categorias de falhas de conexão são:

- Falhas de conexão do cliente — lista as sessões onde ocorreram erros de comunicação no endpoint.
- Falhas da máquina — lista as sessões onde ocorreram erros na máquina.

Além disso, o subpainel de Falhas de conexão exibe as seguintes recomendações para resolver os erros.

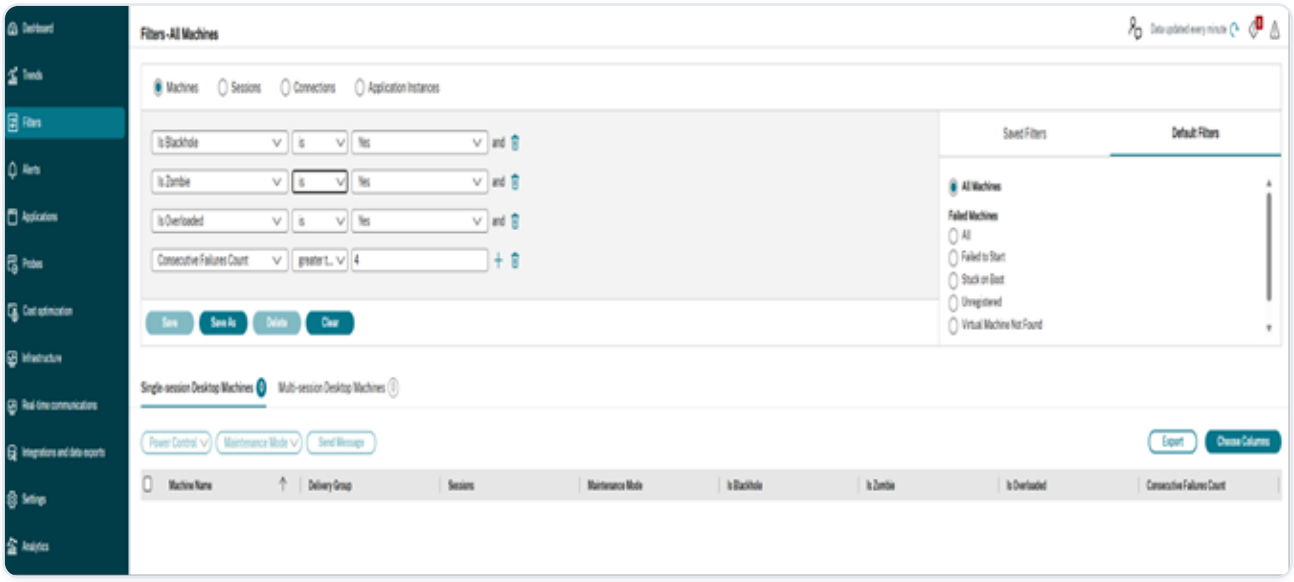
- Verifique as configurações do firewall na máquina e no gateway.
- Verifique a conectividade de rede entre os componentes.
- Certifique-se de que as máquinas estejam ligadas e em estados registrados.

As falhas são agrupadas para identificar usuários bloqueados, ou seja, usuários que não tiveram nenhuma sessão bem-sucedida após a falha de conexão na duração de tempo selecionada. Os padrões são destacados para ambas as categorias de falhas. Clicar nos detalhes abre a visualização Conexões, que é filtrada para mostrar todas as sessões que falharam devido aos erros em seu ambiente durante o tempo selecionado. Esta visualização ajuda a analisar as sessões individuais que falharam e a obter uma possível causa raiz.

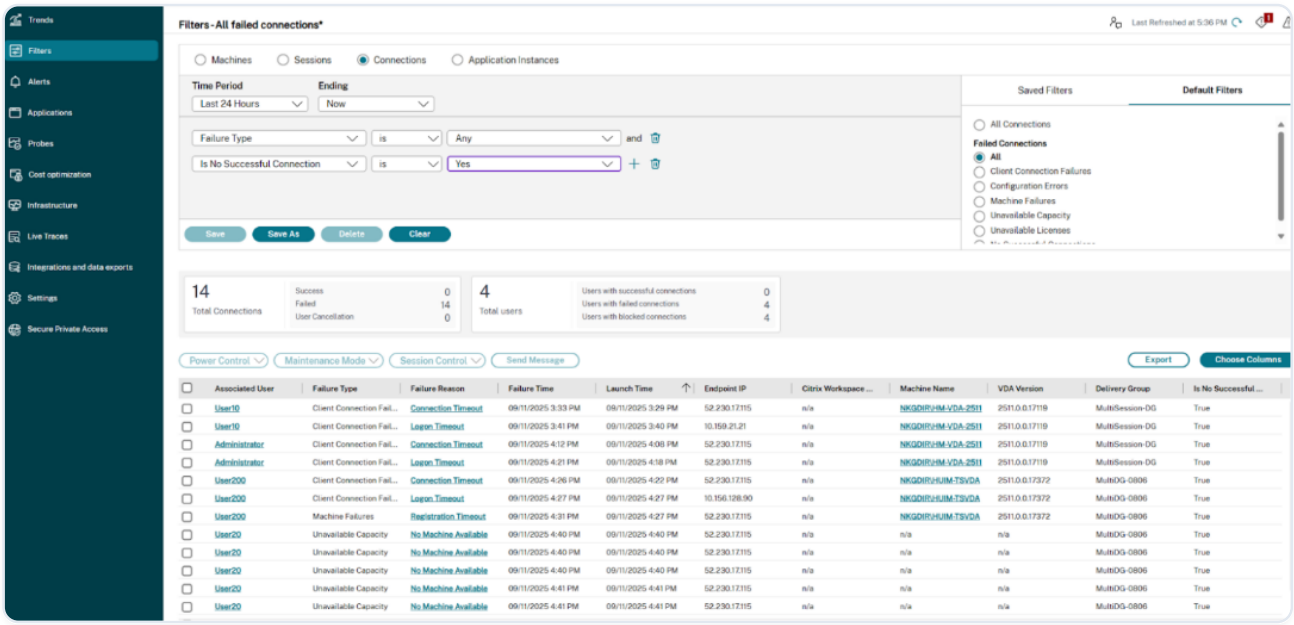
Visualização de Filtro

A seguir estão os novos filtros e colunas que são adicionados à visualização Máquinas em Filtros -> Máquinas:

- Contagem de Falhas Consecutivas: Número de falhas consecutivas de inicialização de sessão que a máquina relatou
- É Blackhole: Se a máquina foi identificada como uma máquina black hole
- É Zumbi: Se a máquina foi identificada como uma máquina zumbi
- Está Sobrecargada: Se a máquina foi identificada como uma máquina sobrecarregada



A seguir estão os novos filtros e colunas que são adicionados à exibição Conexões em Filtros -> Conexões:

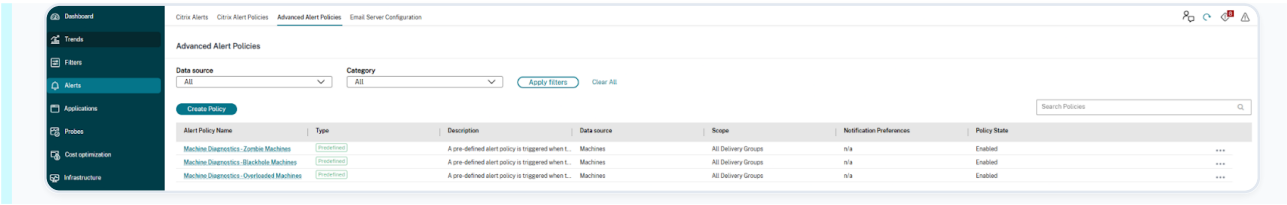


Alertas

Existem 3 novas “Políticas de Alerta Avançadas” que estão disponíveis e habilitadas por padrão para ajudar os administradores a levantar alertas proativamente caso máquinas Black hole, Zumbi ou Sobrecargadas (em todos os grupos de entrega) sejam identificadas no sistema

> **Nota:**

> Falhas de conexão não são suportadas em Políticas de Alerta Avançadas na versão atual.



Gerenciando Políticas Padrão

Para maximizar o valor do Diagnostic Insights, aqui estão alguns pontos-chave sobre as políticas de alerta padrão:

- **Personalização:** Os administradores podem personalizar os **parâmetros da política de alerta, escopo ou ações de notificação** para essas políticas padrão.
- **Restrições:** Você **não pode alterar as condições** ou **excluir** as políticas padrão.
- **Ativar/Desativar:** As políticas podem ser **desativadas ou ativadas** conforme necessário.
- **Notificações:** As políticas padrão **não têm notificações configuradas** de fábrica; elas resultarão apenas em **alertas da interface do usuário**. **Aconselhamos fortemente os administradores a atualizarem as preferências de notificação** nessas políticas.

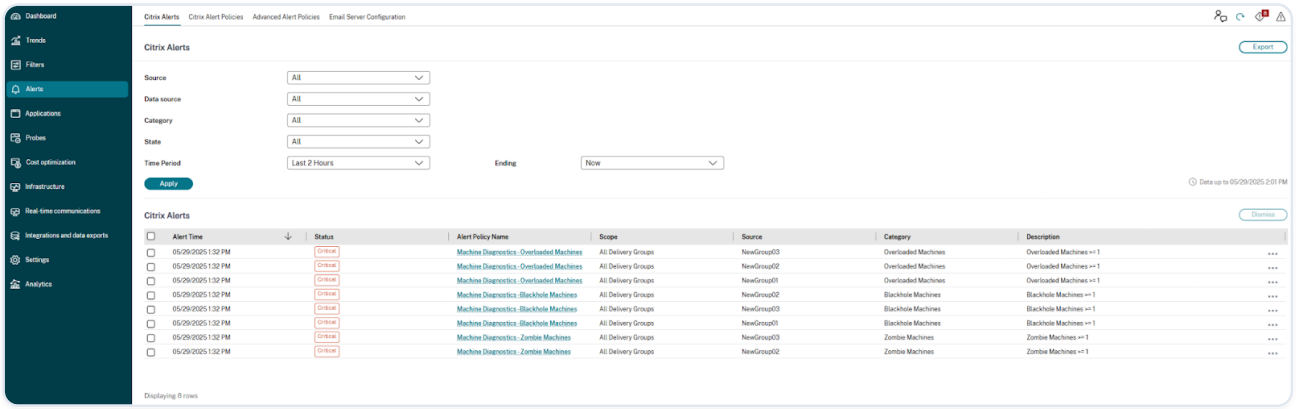
> **Observação:**
>
> - O Painel de Insights em si depende de políticas ativadas. Se você desativar as políticas padrão e não tiver políticas personalizadas ativadas, o Painel de Insights deixará de ser atualizado.
> - A atualização dos parâmetros de alerta também altera o cálculo do insight correspondente no painel.

Criando Políticas Personalizadas

Você pode criar **políticas personalizadas** adicionais para esses insights. Se você criar uma política personalizada, recomendamos **modificar o escopo da política padrão** para **excluir quaisquer Delivery Groups** cobertos pela sua política personalizada. Isso evita sobreposições e possíveis alertas duplicados.

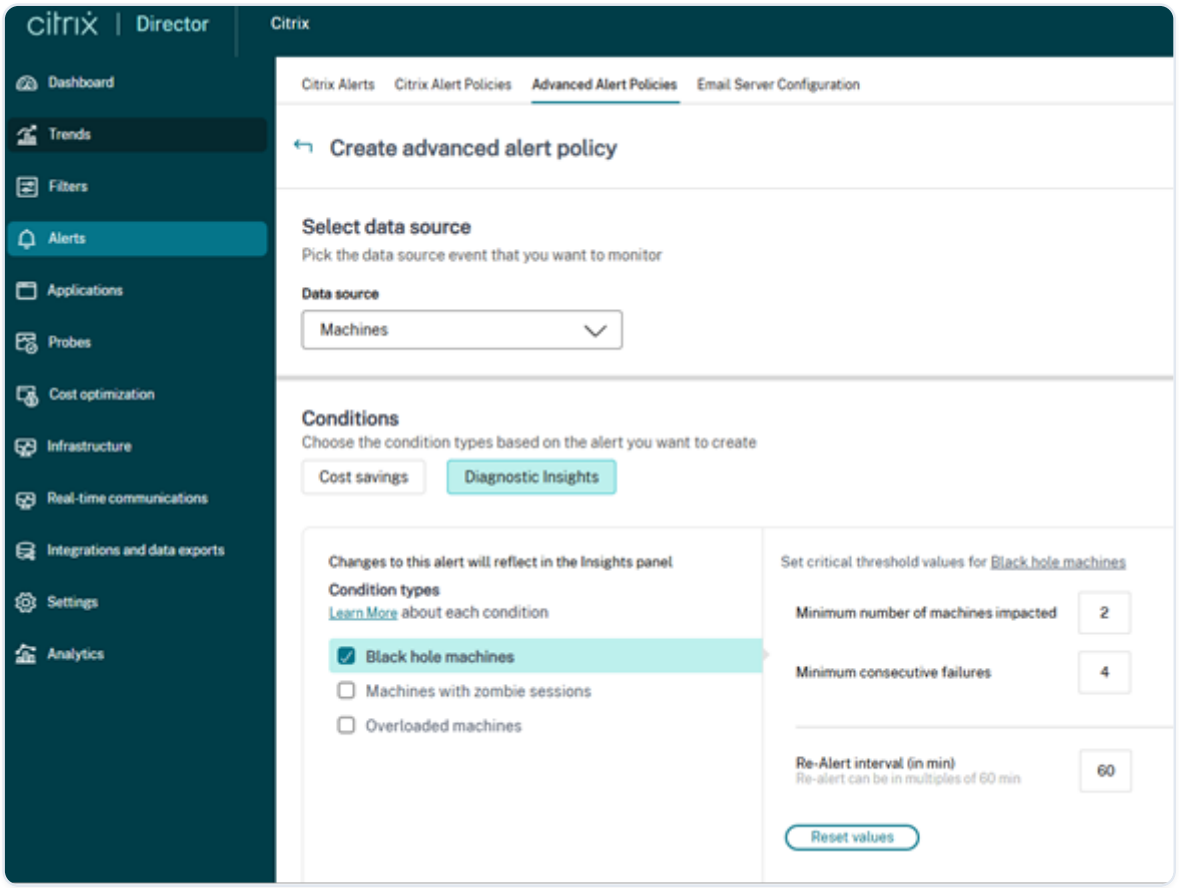
Notificações de alerta

A seguir, uma visão rápida dos ‘Alertas Citrix’ gerados para os insights:



Alerta para Máquinas Black Hole

O Monitor verifica máquinas Black hole a cada 15 minutos e envia um alerta aos administradores para mitigar proativamente as falhas de sessão enfrentadas pelos usuários. Máquinas que falharam ao atender quatro ou mais solicitações de sessão consecutivas são denominadas máquinas Black hole por padrão. As condições de alerta e os intervalos de re-alerta podem ser personalizados para o alerta selecionado.



Os detalhes das máquinas que causaram falhas de sessão são enviados nos e-mails de alerta ou no payload do webhook. A política de alerta de máquinas Black hole deve ser ativada para receber essas notificações.

Alerta para Máquinas com Sessões Zumbis

O alerta de Máquinas com Sessões Zumbis é gerado quando uma nova máquina com uma sessão zumbi é detectada no ambiente em um intervalo de 15 minutos.

Os administradores podem personalizar as condições de alerta para o alerta de Máquinas com Sessões Zumbis.

Alerta avançado de sessões zumbis(/en-us/citrix-daas/media/dir-alert-zombie.png)

Os detalhes das máquinas que causaram as sessões zumbis e as falhas são enviados nos e-mails de alerta ou no payload do webhook.

Alerta para Máquinas Sobrecargadas

Máquinas que experimentaram picos sustentados de CPU, ou alto uso de memória, ou ambos, por intervalos de amostragem configurados, são consideradas sobrecarregadas.

Os administradores podem personalizar as condições de alerta e a preferência de re-alerta para o alerta de Máquinas Sobrecargadas.

Máquinas Sobrecargadas(/en-us/citrix-daas/media/dir-alert-overloaded-machines.png)

Realertas

Para os alertas de insight específicos, o comportamento de notificação dentro do **intervalo de Re-Alerta** configurado é incremental. Se novas máquinas problemáticas forem identificadas durante este intervalo, o e-mail ou webhook de re-alerta **conterá apenas essas novas máquinas**. Um alerta completo, listando todas as máquinas problemáticas para um determinado Grupo de Entrega, será enviado uma vez a cada **intervalo de Re-Alerta** (que é de **24 horas por padrão**).

Visualização de Mapa Geográfico

Visão geral

A visualização de Mapa no Citrix Director fornece aos administradores uma visualização geográfica abrangente de lançamentos de sessão bem-sucedidos em seu ambiente Citrix. Este recurso mapeia visualmente as conexões de usuário em escala global, ajudando as equipes de TI a identificar rapidamente padrões de desempenho regionais, solucionar problemas de conectividade geográfica e otimizar a experiência do usuário final com base em dados de localização. O mapa exibe pontos de conexão codificados por cores que indicam o desempenho de logon em diferentes localizações geográficas.

Pré-requisitos

A tabela a seguir lista os recursos, métricas de endpoint e as versões de produto suportadas:

VDAs

VERSÃO DO VDA PARA WINDOWS	VERSÃO DO VDA PARA MAC	VERSÃO DO VDA PARA LINUX
2411 ou posterior	NA	NA

VERSÃO DO VIRTUAL DELIVERY AGENT	VERSÃO DO CITRIX WORKSPACE APP PARA WINDOWS	VERSÃO DO CITRIX WORKSPACE APP PARA MAC	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA LINUX	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA HTML5	VERSÃO DO APLICATIVO CITRIX WORKSPACE PARA CHROMEOS
2411 ou posterior	2409 ou posterior	2409 ou posterior	2408 ou posterior	2411 ou posterior	2411 ou posterior

Nota:

A política de estúdio 'Endpoint Location Data Collection' deve ser habilitada para acessar e exibir dados de localização no mapa. Certifique-se de que esta política esteja configurada antes de prosseguir.

Principais benefícios

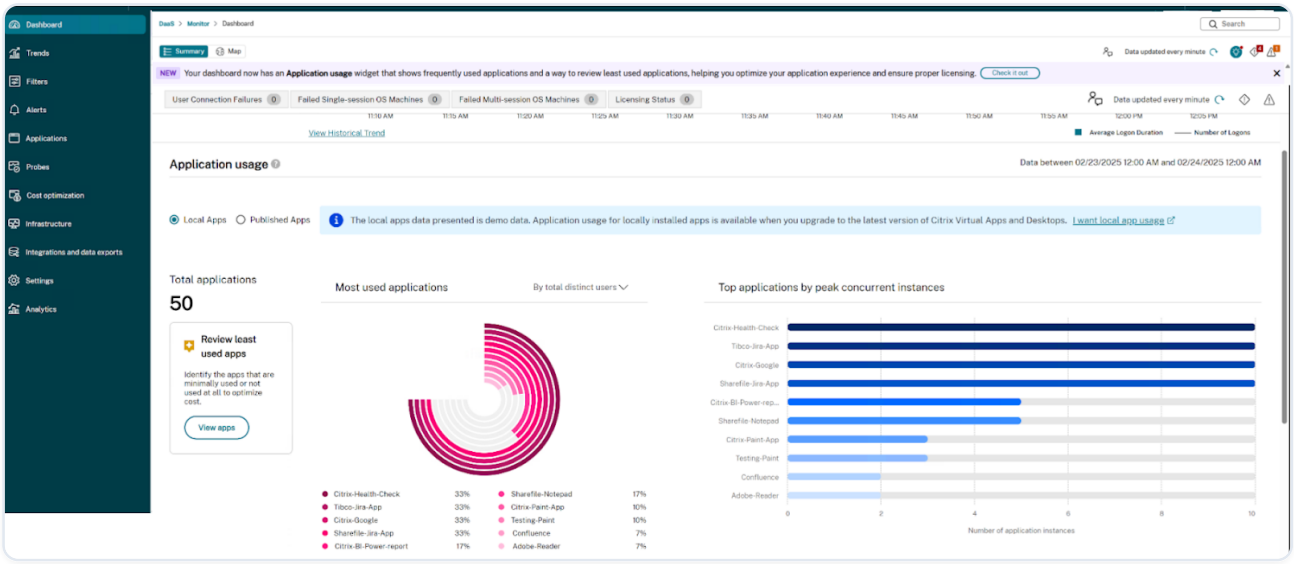
- **Insights de desempenho geográfico:** Visualize instantaneamente as métricas de desempenho da conexão em diferentes países e regiões.
- **Limites de desempenho personalizáveis:** Defina seus próprios padrões para durações de logon baixas, médias e altas (ruins).
- **Visualização da densidade de conexão:** Identifique áreas geográficas de alto tráfego por meio de indicadores codificados por cores e tamanhos de círculo variados.
- **Visão geral da implantação global:** Acesse métricas de resumo críticas para todo o seu ambiente.

- **Solução de problemas regional:** Identifique e resolva rapidamente problemas de desempenho por área geográfica.
- **Monitoramento em tempo real:** Visualize dados que são atualizados automaticamente a cada 5 minutos.

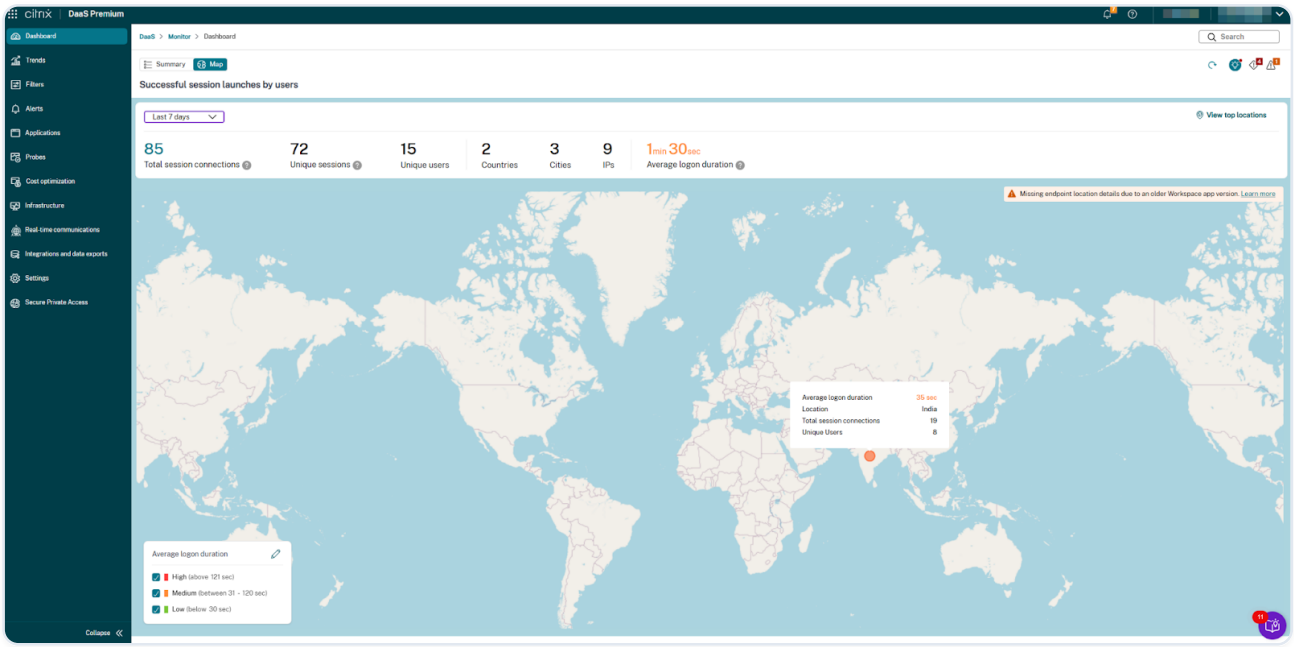
Com permissão total de administrador, ao abrir o Director, o Painel fornece um local centralizado para monitorar a integridade e o uso de um site.

O Painel contém as visualizações Resumo e Mapa:

Visualização de resumo:



Visualização de mapa:



Componentes da interface do usuário

Opções de navegação e visualização

- **Alternância Resumo/Mapa:** Alterne entre estatísticas de resumo e visualização de mapa geográfico
- **Seletor de intervalo de tempo:** Filtre dados por período (padrão: "Última hora")
- **Visualizar principais locais:** Opção para focar em áreas com maior densidade de conexão
- **Indicador de atualização de dados:** Mostra quando os dados foram atualizados pela última vez (atualiza a cada 5 minutos)
- **Ícones de notificação:** Alertas e mensagens do sistema relacionados à implantação

Métricas do painel de resumo

Na parte superior da visualização do Mapa, os administradores podem visualizar as seguintes métricas críticas de toda a implantação:

MÉTRICAS	DESCRIÇÃO
Total de Conexões de Sessão	O número agregado de conexões de sessão em todos os locais
Sessões Exclusivas	O número de sessões individuais estabelecidas, excluindo duplicatas
Usuários Exclusivos	A contagem total de usuários distintos que estabeleceram conexões
Países	O número de países diferentes de onde as conexões se originaram
Cidades	O número de cidades distintas de onde as conexões se originaram
IPs	O número total de endereços IP únicos que estabeleceram conexões
Duração Média do Logon	O tempo médio levado para o estabelecimento da sessão em toda a implantação

Classificação de desempenho

O desempenho da conexão é categorizado nos três níveis a seguir, com limites personalizáveis:

NÍVEL DE DESEMPENHO	CÓDIGO DE CORES	LIMITE PADRÃO	DESCRIÇÃO
Baixo (Bom)	Verde	Abaixo de 60 seg	Experiências de logon rápidas com atrasos mínimos
Médio	Laranja	61-120 seg*	Tempos de logon aceitáveis
Alto (Ruim)	Vermelho	Acima de 120 seg	Experiências de logon abaixo do ideal que exigem atenção

> **Nota:**

> A interface permite que os administradores personalizem esses limites por meio de campos de entrada no painel da legenda.

Legenda do mapa e controles de limite

O painel de legenda interativo fornece:

- **Indicadores de desempenho codificados por cores** com valores de limite correspondentes
- **Campos de limite editáveis** para personalizar o intervalo de desempenho Médio (valores mínimo e máximo)
- **Mensagem de validação** garantindo que o limite máximo exceda o limite mínimo e não seja zero nem negativo
- **Controles de seleção/filtro** para focar em categorias de desempenho específicas

Requisitos do sistema e notificações

Compatibilidade da versão do aplicativo Citrix Workspace

O mapa exibe um banner de aviso quando os detalhes de localização do endpoint estão ausentes devido a versões desatualizadas do aplicativo Citrix Workspace:

- **Mensagem de aviso:** "Detalhes de localização do endpoint ausentes devido a uma versão mais antiga do aplicativo Workspace."
- **Resolução:** A atualização para a versão mais recente do aplicativo Workspace garante a coleta completa de dados geográficos
- **Saiba mais:** O banner inclui um link para a documentação com informações adicionais sobre os requisitos de versão

Opções de configuração

Definindo limites de desempenho

- Localize o painel da legenda no canto inferior esquerdo da visualização do Mapa.
- Insira valores personalizados para a categoria de desempenho Médio:
  - Limite mínimo (padrão: 61 seg)
  - Limite máximo (padrão: 120 seg)
  - A categoria Baixa se ajusta automaticamente para "abaixo de ".
  - A categoria Alta se ajusta automaticamente para "acima de ".
  - A validação garante que o limite máximo exceda o limite mínimo e que nenhum seja zero ou negativo.
  - Valores de limite alterados são armazenados no cache do navegador (armazenamento local) e são específicos do navegador.

Configuração do intervalo de tempo

1. Use o menu suspenso no canto superior esquerdo da seção de métricas.
2. Selecione o período de tempo desejado (padrão: "Última hora").

O mapa e as métricas são atualizados automaticamente para refletir os dados do período selecionado.

Uso da visualização do mapa

Você pode usar a visualização do Mapa para o seguinte:

Solução de problemas de desempenho regional

1. Identifique regiões que mostram predominantemente indicadores de duração de logon vermelhos (Altos).

2. Correlacione com os componentes de infraestrutura que atendem a essas regiões.
3. Implemente otimizações direcionadas para as áreas geográficas afetadas.

Planejamento de capacidade

1. Revise os padrões de densidade de conexão observando os tamanhos dos círculos em diferentes regiões.
2. Identifique áreas geográficas de alto tráfego (círculos maiores) que exigem recursos adicionais.
3. Planeje o dimensionamento da infraestrutura com base nos padrões de uso regional.

Avaliação de implantação global

1. Use o painel de métricas para entender a escala da sua implantação (total de conexões, usuários únicos).
2. Compare o desempenho de logon em diferentes regiões geográficas.
3. Estabeleça expectativas de desempenho de linha de base para diferentes locais.

Otimização de limite

1. Revise a distribuição de indicadores verdes, laranjas e vermelhos no mapa.
2. Ajuste os limites para refletir melhor o desempenho aceitável para seu ambiente específico.
3. Crie uma categorização de desempenho mais significativa com base na experiência real do usuário.

Solução de problemas

Dados geográficos ausentes

Se o banner de aviso "Detalhes de localização do endpoint ausentes devido a uma versão mais antiga do aplicativo Workspace" aparecer:

1. Identifique usuários com versões desatualizadas do aplicativo Citrix Workspace.
2. Planeje uma atualização faseada para a versão mais recente do aplicativo Citrix Workspace.
3. Priorize as atualizações em regiões onde os dados geográficos são mais críticos.

Problemas de categorização de desempenho

Se as categorias de desempenho parecerem representadas de forma imprecisa:

1. Revise as configurações de limite atuais no painel da legenda
2. Ajuste os valores mínimo e máximo da categoria Média conforme necessário
3. Garanta que os limites se alinhem com as características e expectativas de desempenho reais do seu ambiente

Problemas de atualização de dados

Se os dados parecerem desatualizados:

1. Verifique o indicador Dados atualizados a cada 5 minutos para a última hora de atualização.

> **Nota:**
>
> Na última semana, a atualização automática está desabilitada. Atualize manualmente para obter os dados mais recentes.

1. Verifique se o intervalo de tempo selecionado corresponde ao seu período de solução de problemas.
2. Use o botão Atualizar, se disponível, para atualizar os dados manualmente.

Melhores práticas

- Revise e ajuste regularmente os limites de desempenho com base nas melhorias de infraestrutura.
- Use a opção **Ver principais locais** para focar nas áreas com o maior volume de conexão.
- Compare os padrões de desempenho geográfico antes e depois das alterações na infraestrutura.
- Crie relatórios de linha de base de desempenho regional durante períodos de operação ideais.
- Considere as condições da rede regional ao definir as expectativas de desempenho.
- Eduque os usuários sobre a atualização para a versão mais recente do aplicativo Citrix Workspace para coleta completa de dados.
- Verifique regularmente a **Visualização do Mapa** para identificar tendências emergentes no desempenho da sessão.

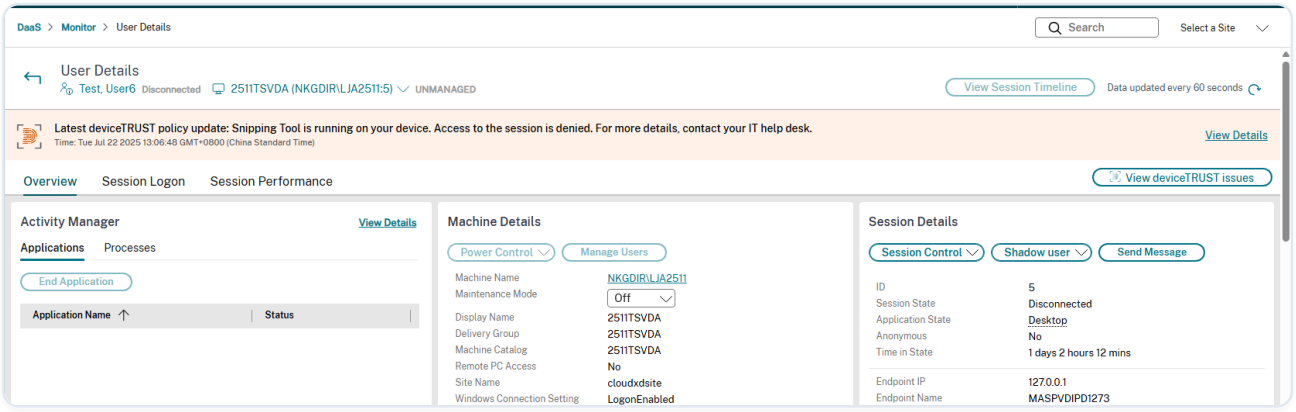
Integração do deviceTRUST® no Monitor

A integração do deviceTRUST® traz informações de segurança contextuais diretamente para o Monitor. Esse recurso é visível apenas quando os componentes do deviceTRUST estão instalados e configurados em seu ambiente Citrix Virtual Apps and Desktops™.

O deviceTRUST monitora continuamente o contexto do dispositivo e garante que os dispositivos remotos que se conectam ao seu ambiente Citrix atendam às políticas de segurança da sua organização. Se um dispositivo não estiver em conformidade, o deviceTRUST pode tomar medidas automaticamente, como desconectar ou encerrar a sessão.

Interrupções de sessão destacadas na página Detalhes do Usuário

As sessões que foram interrompidas ou encerradas por uma ação do deviceTRUST são destacadas na página **Detalhes do Usuário**. Isso indica que a desconexão foi uma medida de segurança deliberada.

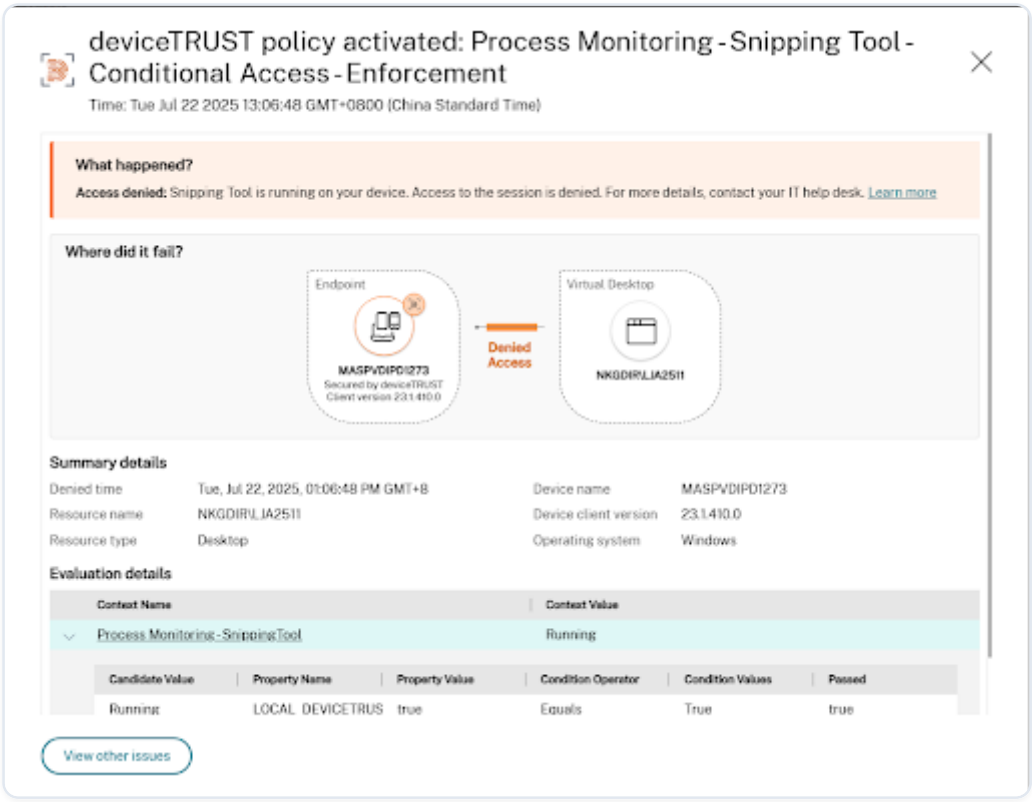


Botão Visualizar problemas do deviceTRUST na página Detalhes do Usuário

Um botão **Visualizar problemas do deviceTRUST** está disponível na página **Detalhes do Usuário**. Clicar neste botão leva o administrador para a guia **Acesso Negado** se houver problemas do deviceTRUST para a sessão nos últimos dois dias. O botão aparece esmaecido se não houver problemas do deviceTRUST para a sessão nos últimos dois dias.

Informações detalhadas de falha do deviceTRUST

Os administradores podem visualizar o motivo exato de uma negação de acesso devido a problemas do deviceTRUST clicando em **Visualizar Detalhes** no banner de problema destacado. Os seguintes detalhes são exibidos:

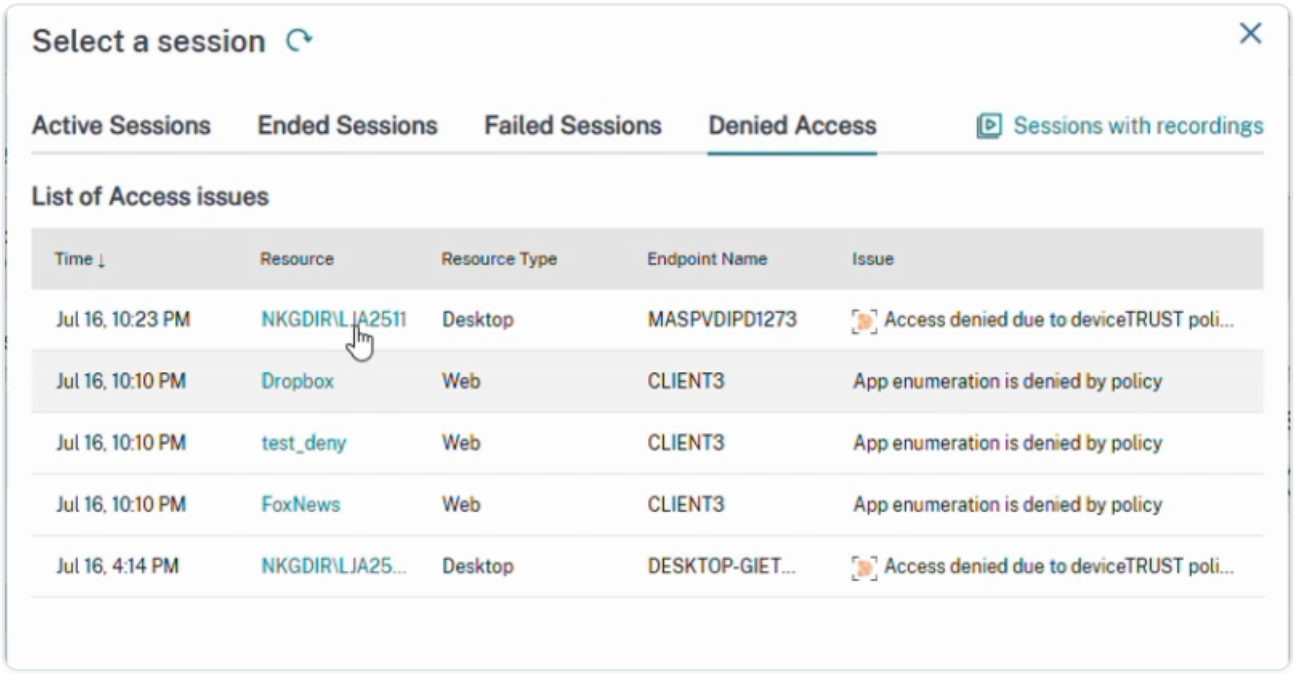


- O motivo da negação de acesso.
- Uma representação visual de onde a conexão foi bloqueada entre o dispositivo de endpoint do usuário e o desktop virtual.
- Detalhes resumidos da negação de acesso, incluindo a hora em que o problema ocorreu, nome do recurso, tipo de recurso, o dispositivo do qual a tentativa de conexão foi feita e a versão do cliente deviceTRUST.
- Detalhes da avaliação da política, incluindo as propriedades e condições que não foram atendidas.

Clique em **Visualizar outros problemas** para navegar até a guia **Acesso Negado**.

Guia Acesso Negado atualizada

A guia **Acesso Negado** foi atualizada para incluir problemas do deviceTRUST. Esta guia fornece uma lista histórica de todos os acessos negados do deviceTRUST e do Secure Private Access. Os administradores podem visualizar informações detalhadas de falha do deviceTRUST clicando em um item do deviceTRUST.



Pontuação da Sessão

Pré-requisitos

A pontuação da sessão via uberAgent lite está disponível a partir da versão 2511 do VDA ou posterior. A capacidade também está sendo retroportada para o LTSR 2507 via CU2.

Visão geral

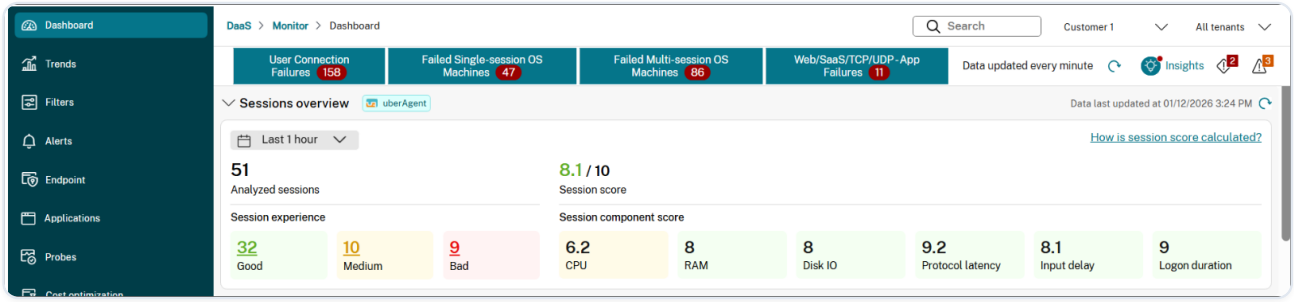
Os detalhes da sessão agora contêm pontos de dados adicionais para solucionar problemas de desempenho da sessão e analisar a integridade geral da sessão. Os dados adicionais fornecem insights sobre a experiência geral do usuário de sessões individuais e ajudam os administradores a entender o motivo das sessões com baixo desempenho.

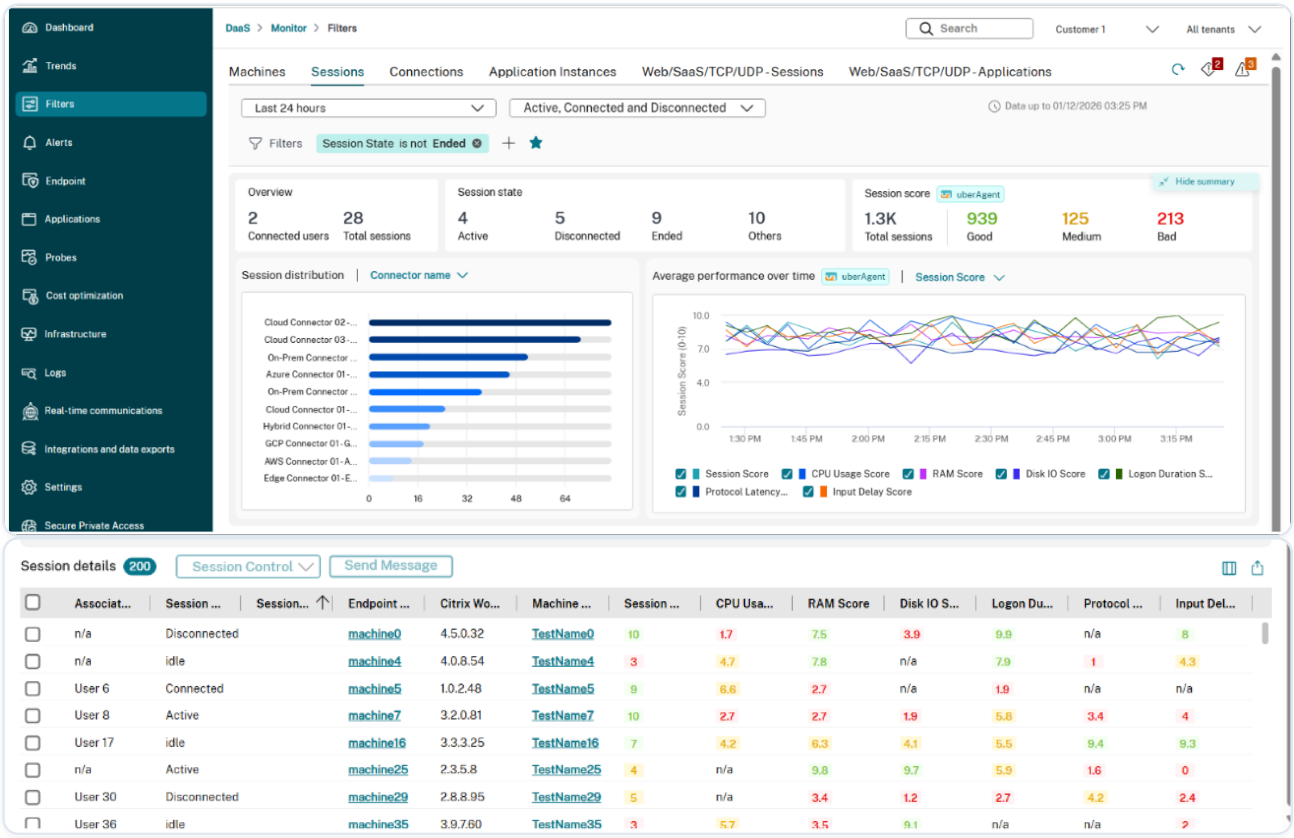
1. Resumo da experiência da sessão – Serve como uma visão rápida da experiência da sessão. Mostra o resumo da experiência do usuário em todas as sessões iniciadas no ambiente durante o período selecionado. As sessões analisadas são categorizadas em Boa, Média e Ruim. Os administradores podem clicar em uma categoria de experiência para abrir a visualização detalhada da sessão (página Filtros) com filtros aplicados automaticamente.
2. Pontuação da sessão e do componente – O resumo da sessão também fornece a pontuação média da sessão e do componente para a sessão analisada. Embora as pontuações médias autônomas possam não ser uma métrica muito útil, elas ainda podem servir como um bom indicador da experiência da sessão para a maioria das sessões. Da mesma forma, o administrador pode usar as pontuações médias dos componentes para entender a causa raiz potencial das sessões ruins.

3. Distribuição da sessão – O gráfico de distribuição da sessão é adicionado à página de filtros. O administrador pode visualizar a distribuição da sessão por País do Endpoint, Cidade, SO do Endpoint, versão do CWA, ISP, etc.
4. Tendências de desempenho – O gráfico de tendências de desempenho da sessão também é adicionado à página de filtros. O gráfico de desempenho é útil para analisar as tendências de desempenho da sessão e dos componentes e identificar quaisquer padrões recorrentes com base na hora do dia, país, etc.
5. Dados de sessão individual – Os seguintes pontos de dados foram adicionados para cada sessão na tabela de detalhes da sessão –

    a. Pontuação da sessão
    b. Pontuação da CPU
    c. Pontuação da RAM
    d. Pontuação de E/S de Disco
    e. Pontuação de Latência do Protocolo
    f. Pontuação de atraso de entrada
    g. Pontuação de duração do logon

Para obter mais informações sobre o cálculo da pontuação de experiência, consulte Pontuação de Experiência.





Session details 200 | Session Control | Send Message

Associat...	Session ...	Session...	Endpoint ...	Citrix Wo...	Machine ...	Session ...	CPU Usa...	RAM Score	Disk IO S...	Logon Du...	Protocol ...	Input Del...
n/a	Disconnected		machine0	4.5.0.32	TestName0	10	1.7	7.5	3.9	9.9	n/a	8
n/a	idle		machine4	4.0.8.54	TestName4	3	4.7	7.8	n/a	7.9	1	4.3
User 6	Connected		machine5	1.0.2.48	TestName5	9	6.6	2.7	n/a	1.9	n/a	n/a
User 8	Active		machine7	3.2.0.81	TestName7	10	2.7	2.7	1.9	5.8	3.4	4
User 17	idle		machine16	3.3.3.25	TestName16	7	4.2	6.3	4.1	5.5	9.4	9.3
n/a	Active		machine25	2.3.5.8	TestName25	4	n/a	9.8	9.7	5.9	1.6	0
User 30	Disconnected		machine29	2.8.8.95	TestName29	5	n/a	3.4	1.2	2.7	4.2	2.4
User 36	idle		machine35	3.9.7.60	TestName35	3	5.7	3.5	9.1	n/a	n/a	2

Visibilidade da Versão do SO do Endpoint

As páginas de **Sessão** e **Conexão** incluem uma coluna **Versão do SO do Endpoint** e um filtro correspondente. A coluna permite visualizar a versão do sistema operacional do endpoint. Você pode filtrar sessões ou conexões com base na versão do SO a partir da qual o usuário inicia. Este recurso suporta dispositivos Windows e Linux.

Vantagens

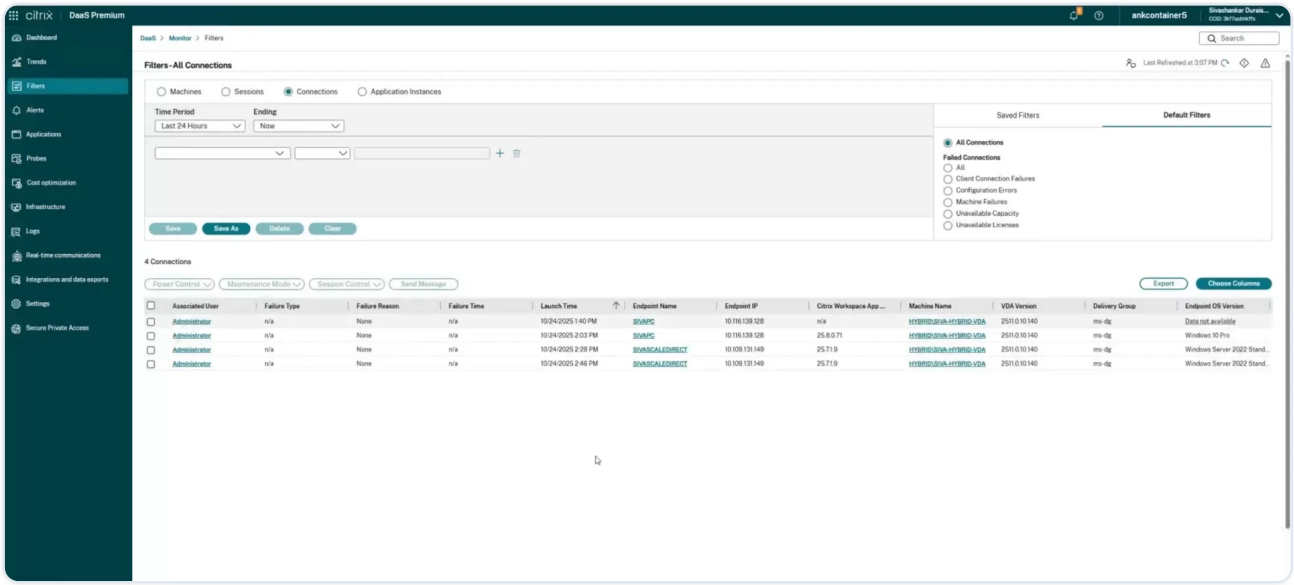
- Visualize a versão do SO do endpoint nas páginas de **Sessão** e **Conexão**.
- Filtre sessões ou conexões com base na versão do SO do endpoint.

Exemplo de uso

Para filtrar sessões ou conexões iniciadas a partir de uma versão específica do SO Windows:

1. navegar para a página **Sessões** ou **Conexões**.
2. Localize o filtro para a coluna **Versão do SO do Endpoint**.
3. Insira o texto específico para a versão do Windows pela qual você deseja filtrar (por exemplo, `Windows 10`).
4. Aplique o filtro.

Exemplo: Se você inserir `Windows 10` no filtro, a lista será atualizada para mostrar apenas as conexões ou sessões iniciadas a partir de máquinas Windows 10.



Aplicabilidade

- Dispositivos Windows
- Dispositivos Linux

Requisitos do sistema

- **Versão Mínima do Aplicativo:**
  - Versão do aplicativo CWA para Windows: 2508
  - Versão do aplicativo CWA para Linux: CWAL 2601
- **Versão Mínima do VDA:** Versão do VDA 2511

Limitações

A coluna **Versão do SO do Endpoint** exibe valores apenas para dispositivos Windows e Linux. Outros sistemas operacionais não são atualmente suportados. O suporte para outros sistemas operacionais está planejado para futuras versões.

Ativação da política de segurança de endpoint e relatórios de detecção de ameaças

O Citrix Workspace App está introduzindo verificações de segurança integradas que detectarão automaticamente condições de alto risco, como o Microsoft Recall habilitado em endpoints, sem a

necessidade de qualquer configuração manual. Essa visibilidade em tempo real de tais detecções estará disponível no Citrix Monitor e no Monitor. Os relatórios permitirão que os administradores avaliem rapidamente o risco e configurem suas políticas de proteção para garantir um ambiente mais seguro. Embora a detecção de eventos selecionados como o Recall seja automática, a proteção contra eventos requer a configuração manual de políticas de proteção de aplicativos pelo administrador. Os eventos de ativação para todas as políticas habilitadas também serão relatados no Monitor e no Monitor. Ao utilizar o gerenciamento proativo de riscos e a reconfiguração de políticas, os administradores poderão fortalecer a segurança dos endpoints em seu ambiente e reduzir a exposição a ameaças emergentes.

Os seguintes relatórios estarão disponíveis no Monitor:

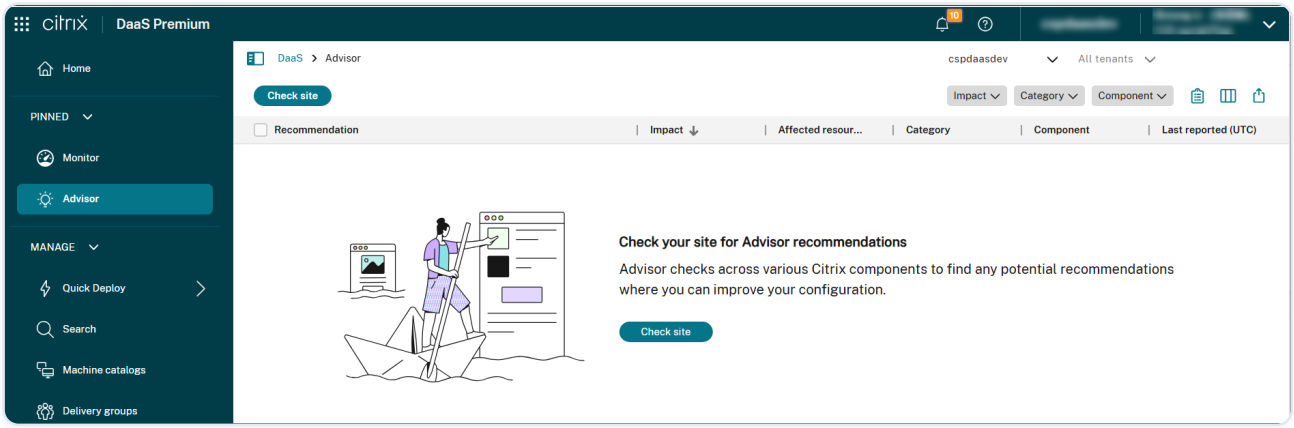
- **Trilha de Auditoria**
    - **Detecção Automática** – Durante sua varredura padrão, o CWA detecta várias ameaças, como o Windows Recall no endpoint. Se uma ameaça for detectada, o CWA enviará um evento para o Monitor. Os seguintes dados serão relatados para cada evento –
        - Carimbo de data/hora
        - Nome de usuário
        - Nome do endpoint
        - SO do endpoint
        - Versão do CWA
        - Nome do evento
        - Tipo de evento – Detecção ou proteção
- **Proteção para políticas configuradas** – Os administradores podem configurar políticas de proteção para evitar certos eventos, como captura de tela, injeção de DLL ou registro de teclas. A política de proteção contra captura de tela também pode ser usada para evitar tentativas de captura de tela pelo Recall. Os eventos de proteção relatados no Monitor incluirão todos os pontos de dados listados acima.
- **Insights e tendências agregados** – Os dados de eventos serão agregados para relatar as seguintes informações:
    - Resumo de detecção/proteção para o ambiente,
    - Principais eventos protegidos/detectados e
    - Tendência de eventos de proteção e detecção ao longo do tempo

Essa capacidade foi projetada para fortalecer ainda mais o compromisso da Citrix de entregar aplicativos com segurança, ajudando as organizações a identificar ameaças emergentes e a respondê-las em tempo real.

Os administradores podem usar os insights acima para entender melhor as “ameaças” de segurança em seu ambiente e configurar políticas de proteção para proteger dados confidenciais, minimizar riscos de segurança e apoiar o estabelecimento de políticas corporativas relacionadas projetadas para mitigar tais riscos. (por exemplo, desencorajar o uso de ferramentas como recall, keylogger, etc.)

Advisor

O Citrix Advisor é um serviço que ajuda a otimizar a implantação do DaaS e a aprimorar sua saúde e prontidão gerais. Ele automatiza verificações de ambiente e fornece recomendações acionáveis, capacitando você a identificar proativamente problemas de configuração, ineficiências, desperdícios de recursos, desvios das melhores práticas e muito mais.



Nota:

- Este serviço está disponível exclusivamente para **Administradores Completos**.
- Recomendamos enviar seu feedback usando o ícone de feedback no canto superior direito da página.

Benefícios

Com o Advisor, você pode:

- **Identificar e resolver problemas proativamente**: Detectar problemas potenciais, desvio de configuração e desvios das melhores práticas antes que eles afetem os usuários, interrompam as operações de negócios ou comprometam a segurança.
- **Otimizar o desempenho e a estabilidade do ambiente**: Ajustar configurações, otimizar a alocação de recursos e implementar as melhores práticas para aprimorar a estabilidade, segurança e desempenho de suas implantações Citrix.

- **Simplificar operações e reduzir a sobrecarga**: Automatizar verificações de rotina, simplificar tarefas complexas de remediação e receber assistência guiada, reduzindo assim a sobrecarga operacional e liberando recursos administrativos.
- **Otimizar custos e utilização de recursos**: Identificar áreas de gastos excessivos, descobrir oportunidades de otimização de recursos e garantir a utilização eficiente das tecnologias Citrix para minimizar o custo total de propriedade.
- **Manter a conformidade e a adesão às melhores práticas**: Garantir que suas implantações Citrix sigam as melhores práticas da Citrix, padrões de segurança e regulamentações da indústria, reduzindo riscos e melhorando a governança geral.
- **Simplificar tarefas complexas**: Simplificar tarefas administrativas para suportar um ambiente saudável e otimizado.

Verificar recomendações

O Advisor executa automaticamente verificações de site em um agendamento semanal recorrente (domingos às 2:00 AM UTC), fornecendo uma visão regularmente atualizada da integridade do seu ambiente. Cada execução gera um relatório retido por até 90 dias e depois automaticamente limpo. As recomendações da execução agendada mais recente aparecem na página **Advisor** e no widget **Advisor** na página **Home**.

Você também pode executar uma verificação de site manualmente a qualquer momento. Uma verificação manual atualiza a recomendação imediatamente, independentemente do ciclo de execução agendado.

Para executar uma verificação de site manual, siga estas etapas:

1. Faça login no Citrix Cloud usando uma conta com a função de **Administrador Completo**.
2. Clique no bloco **DaaS**.
3. No painel esquerdo, selecione **Advisor**.
4. Clique em **Verificar site**.
5. Na página **Verificar site**, selecione as categorias que você deseja que o Advisor verifique.

CATEGORIA	DESCRIÇÃO	REFERÊNCIA
Segurança	Recomendações para detectar ameaças e vulnerabilidades que podem	Recomendações de segurança

CATEGORIA	DESCRIÇÃO	REFERÊNCIA
	levar a violações de segurança.	
Confiabilidade	Recomendações para garantir e melhorar a continuidade de seus aplicativos críticos para os negócios.	Recomendações de confiabilidade
Desempenho	Recomendações para aprimorar o desempenho em aplicativos e desktops para oferecer experiências mais rápidas e responsivas aos usuários finais.	Recomendações de desempenho
Excelência operacional	Recomendações para ajudar você a alcançar eficiência de processo e fluxo de trabalho, capacidade de gerenciamento de recursos e melhores práticas de implantação.	Recomendações de excelência operacional
Otimização de custos	Recomendações para reduzir os gastos gerais, dimensionando corretamente os recursos, minimizando o desperdício e alinhando a capacidade com as necessidades reais de uso.	Recomendações de otimização de custos

6. Clique em **Executar verificação** para executar uma verificação do site e gerar recomendações atualizadas com base na configuração atual.

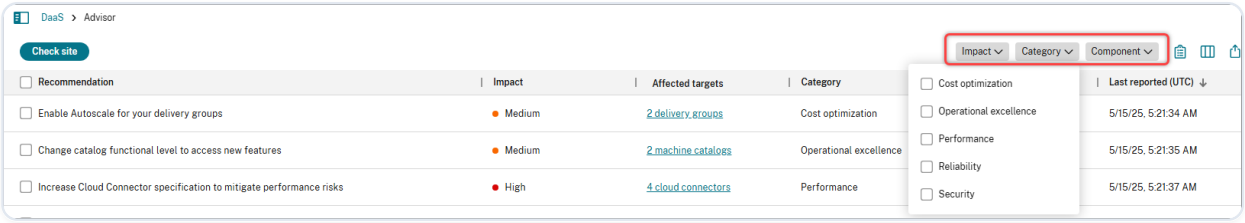
   Todas as recomendações aparecem na lista.



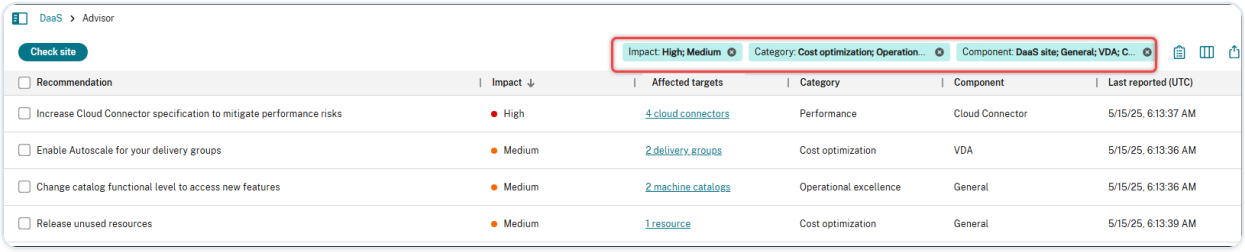
Filtrar recomendações

Você pode filtrar as recomendações por **Impacto**, **Categoria** ou **Componente** para focar nas informações mais relevantes para sua implantação.

1. No **Advisor**, localize os filtros no canto superior direito da lista de recomendações.



2. Clique em um filtro (por exemplo, **Categoria**) para ver as opções disponíveis.
3. Selecione uma ou mais caixas de seleção para aplicar o filtro. A lista é atualizada automaticamente para exibir apenas as recomendações que correspondem às suas seleções.
4. Use vários filtros juntos para refinar a lista.



Revisar e agir sobre as recomendações

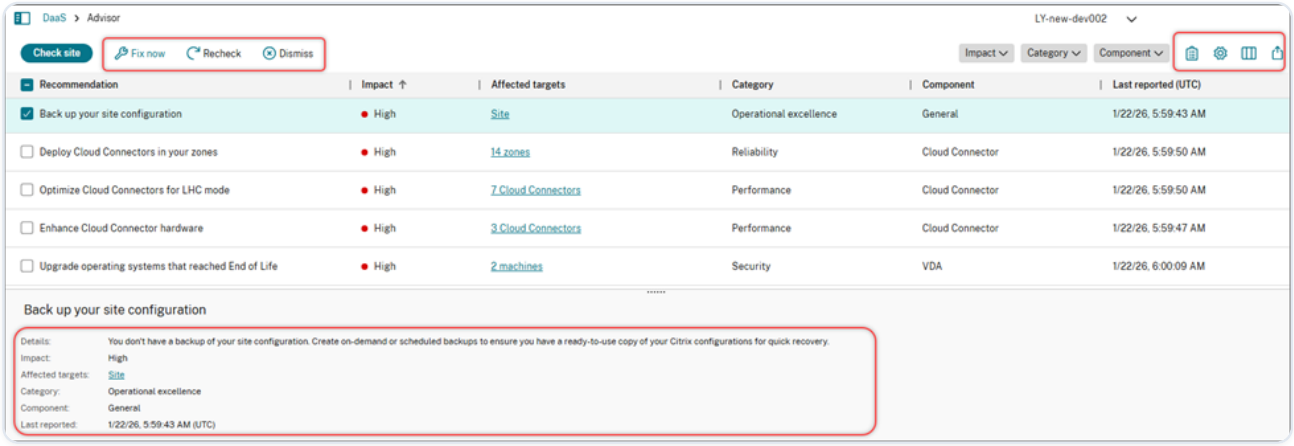
Use a lista de recomendações para entender os problemas de configuração e as oportunidades de melhoria em sua implantação. Você pode realizar as seguintes ações nas recomendações:

- Exibir detalhes da recomendação
- Implementar ações recomendadas
- Descartar recomendações
- Descartar alvos afetados específicos em uma recomendação
- Personalizar regras de verificação

- Exibir o relatório completo de verificação do site

Ver detalhes da recomendação

Para revisar uma recomendação, selecione uma recomendação para visualizar seus detalhes no painel inferior.

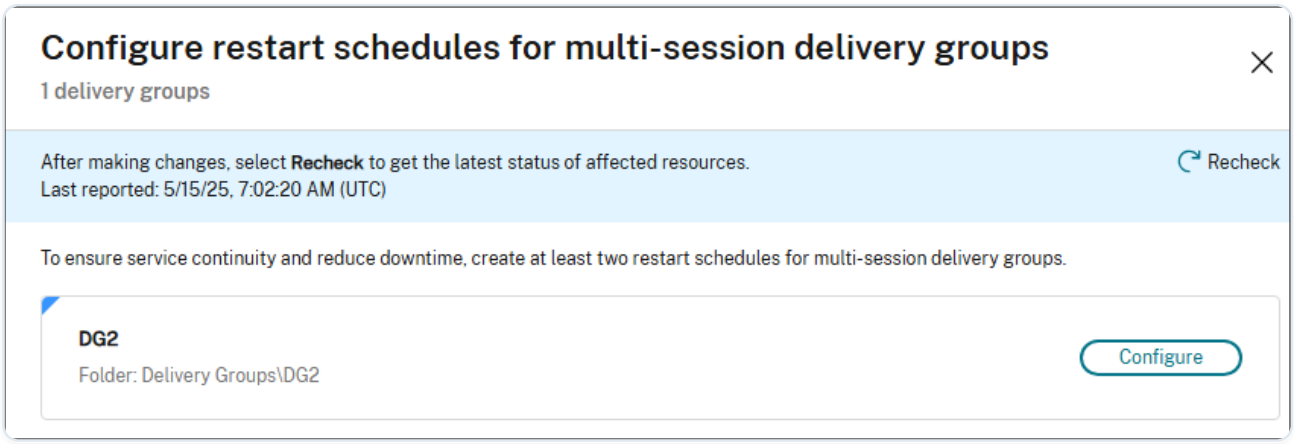


Implementar ações recomendadas

Para implementar as ações recomendadas para uma recomendação, siga estas etapas:

1. Selecione uma recomendação.
2. Clique em **Corrigir agora** na barra de ações.
3. Siga as etapas recomendadas para fazer as atualizações necessárias.

   Às vezes, você é direcionado à documentação de suporte quando a configuração automatizada não é suportada ou viável. Queremos garantir que o Advisor seja projetado para fornecer ações automatizadas diretamente na interface do usuário sempre que possível, minimizando a necessidade de configuração manual.
4. Após fazer as atualizações, clique em **Verificar novamente** para atualizar o status dos destinos afetados.



> **Nota:**
>
> A interface do usuário e as etapas variam dependendo da recomendação. A captura de tela mostrada é apenas para fins ilustrativos.

Descartar recomendações

Se uma recomendação não for relevante para sua implantação ou não exigir ação, você poderá removê-la da lista atual e dos resultados de verificações futuras:

1. Selecione a recomendação.
2. Clique em **Ignorar** na barra de ações.

> **Dica:**
>
> Para restaurar um destino ignorado em uma recomendação, clique no ícone de **Engrenagem** no canto superior direito acima da lista de recomendações e selecione **Gerenciar itens ignorados**

Ignorar destinos afetados específicos em uma recomendação

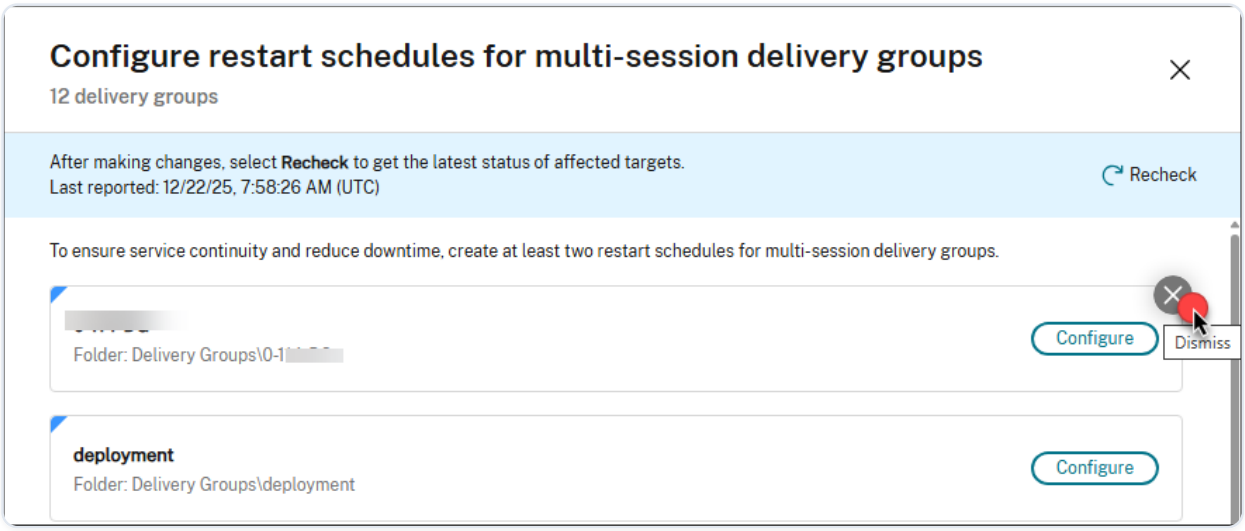
Se uma recomendação incluir destinos afetados que intencionalmente não estão em conformidade com as melhores práticas (*por exemplo*, recursos de teste, validação ou temporários), você pode removê-los desta recomendação (ignorar granularmente).

> **Observação:**
>
> A ignorância granular é suportada apenas para os seguintes destinos: catálogos de máquinas, grupos de entrega, grupos de aplicativos e zonas.

> As etapas detalhadas são as seguintes:

1. Selecione a recomendação.
2. Clique no campo **Destinos afetados** da recomendação. A página de recomendação exibe todos os destinos afetados.

3. Passe o mouse sobre o destino afetado que você deseja ignorar. Um ícone de **Ignorar** aparece no canto superior direito do destino.



4. Clique no ícone de **Ignorar**. Uma caixa de diálogo de confirmação de ignorância aparece.
5. Insira uma nota para a ignorância, se necessário, e, em seguida, clique em **Ignorar**. O destino afetado é removido da página de recomendação.

> **Dica:**
>
> Para restaurar um destino ignorado em uma recomendação, clique no ícone de Engrenagem no canto superior direito acima da lista de recomendações e selecione **Gerenciar itens ignorados**.

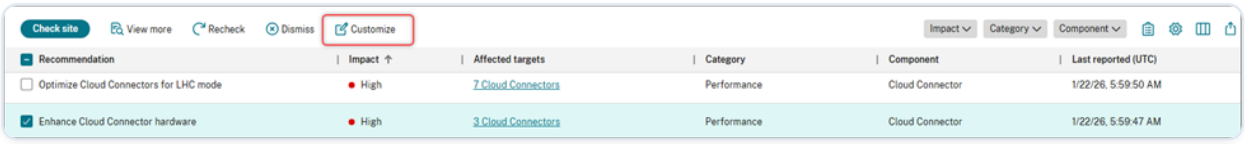
Personalizar regras de verificação

Você pode personalizar as regras de verificação do Advisor para as seguintes recomendações:

- **Aprimorar o hardware do Cloud Connector:** Ajuste os limites de uso de CPU, memória e disco, e exclua discos específicos.
- **Liberar recursos não utilizados:** Defina limites de tempo de inatividade personalizados para máquinas e aplicativos.
- **Otimizar a configuração de GPO para VDAs:** Modifique o limite de tempo de processamento de GPO.

Para personalizar a regra de verificação para uma única recomendação, siga estas etapas:

1. Selecione uma recomendação e clique em **Personalizar** na barra de ações.



2. Na página **Personalizar**, atualize as configurações de verificação conforme necessário.
3. Clique em **Salvar**. As alterações entrarão em vigor na próxima vez que você executar a verificação.

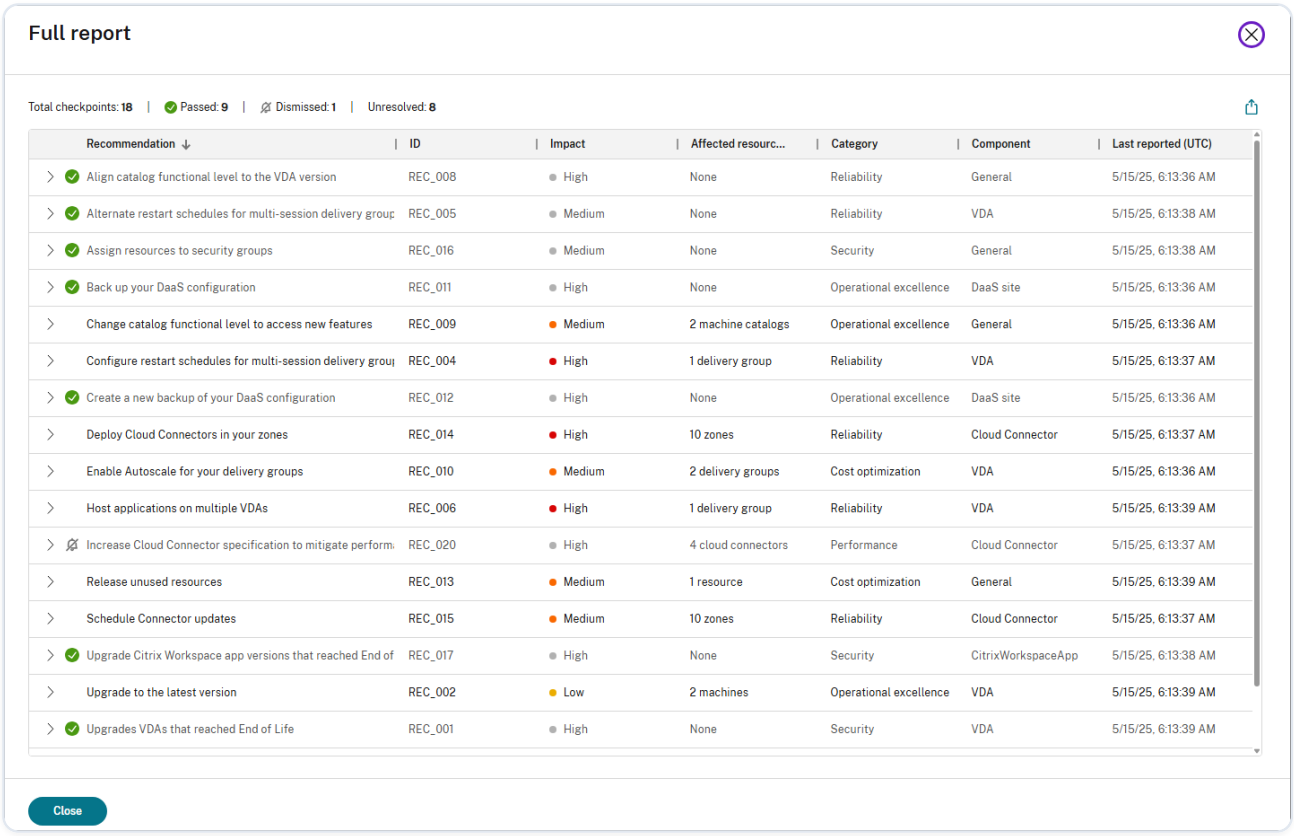
Para personalizar as regras de verificação para todas as três recomendações a partir de um local central, siga estas etapas:

1. Clique no ícone de **Engrenagem** no canto superior direito acima da lista de recomendações e selecione **Personalizar regras**. As três recomendações aparecem.
2. Clique no ícone de **Editar** ao lado de uma recomendação.
3. Atualize as configurações da verificação conforme necessário.
4. Para atualizar as regras de verificação para as recomendações restantes, repita as etapas 2 a 3.
5. Clique em **Salvar**. As alterações entrarão em vigor na próxima vez que você executar a verificação.

Visualizar o relatório completo de verificação do site

O **relatório completo** fornece um resumo de todas as recomendações do Advisor da verificação mais recente do site. Ele inclui pontos de verificação aprovados, ignorados e não resolvidos, ajudando você a avaliar a saúde geral e as oportunidades de otimização em seu site DaaS.

Para visualizar o relatório completo, clique no ícone **Visualizar relatório completo** no canto superior direito da lista de recomendações.



Configurar o StoreFront para verificação do Advisor

As recomendações relacionadas ao StoreFront no Citrix Advisor exigem configuração adicional. Para configurar o StoreFront para verificações do Advisor, conclua as seguintes etapas:

1. Adicione seus servidores StoreFront ao Infrastructure Monitoring criando as conexões correspondentes. Para obter mais informações, consulte Configuração do Infrastructure Monitoring.
2. Se você configurar uma conexão StoreFront no modo **Conexão manual**, certifique-se de que o Citrix Infrastructure Monitoring versão 2603 ou posterior esteja baixado e instalado. Para verificar se uma versão necessária está instalada:
    a. Vá para **Monitor > Configurações**.
    b. Localize a conexão onde **Tipo** é igual a `StoreFront`.
    c. Confirme se o campo **Versão** exibe `7.47` ou superior.

> **Importante:**
>
> Depois de aplicar as alterações à sua implantação do StoreFront com base nas recomendações do Advisor, aguarde pelo menos 6 horas antes de verificar novamente as

> mesmas recomendações. Esse atraso permite que o Monitoramento de Infraestrutura colete e processe telemetria atualizada e garante que o Advisor avalie os dados mais recentes.

Referências

Esta seção lista todas as recomendações do Citrix Advisor por categoria para ajudar você a entender seu propósito e impacto.

Recomendações de segurança

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
Atualizar VDAs que atingiram o Fim da Vida Útil	REC_001	Alto	VDA	Algumas máquinas estão usando versões de VDA que atingiram o Fim da Vida Útil e não são mais suportadas pela Citrix. Atualize as máquinas afetadas para a versão VDA LTSR ou CR mais recente.
Atribuir recursos a grupos de segurança	REC_016	Médio	Geral	Alguns recursos são atribuídos a usuários individuais. É uma prática recomendada da Citrix atribuir acesso de usuário apenas por meio de grupos de segurança para otimizar o

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				gerenciamento e aprimorar a segurança. Reconfigure a atribuição de usuário para grupos de entrega e aplicativos para incluir apenas grupos de segurança.
Atualize as versões do aplicativo Citrix Workspace que atingiram o Fim da Vida Útil	REC_017	Alta	Aplicativo Workspace	Alguns dispositivos de endpoint usam uma versão do aplicativo Citrix Workspace que atingiu o Fim da Vida Útil. Atualize os dispositivos para a versão mais recente do aplicativo Workspace para reduzir a capacidade de suporte e os riscos de segurança. Para gerenciamento de versão simplificado e controle de atualização automática, use o Serviço de

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				Configuração Global de Aplicativos. Além disso, considere usar soluções de análise de endpoint para impor uma versão mínima do aplicativo Workspace para acessar a loja.
Implementar políticas de postura de dispositivo	REC_021	Médio	Acesso Privado Seguro	A configuração atual do Acesso Privado Seguro não possui políticas de postura de dispositivo, permitindo acesso irrestrito a aplicativos internos de qualquer dispositivo. Para mitigar esse risco e aprimorar a segurança, implemente políticas de postura de dispositivo que classifiquem os dispositivos como: **Conforme**,

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				Não conforme e **Acesso negado**.
Implementar políticas de acesso adaptativo	REC_022	Médio	Acesso Privado Seguro	A configuração atual do Acesso Privado Seguro não possui políticas de acesso adaptativo, permitindo acesso potencialmente inseguro a aplicativos. Para aumentar a segurança, implemente políticas de acesso adaptativo que controlem dinamicamente o acesso a aplicativos web corporativos, SaaS, TCP e UDP com base no contexto. Para controles granulares, habilite o acesso restrito a aplicativos web corporativos e SaaS adicionando as restrições de

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				segurança: **Área de transferência**, **Captura de tela**, **Impressão**, **Proteção contra registro de teclas**, **Downloads**, **Uploads**, **Marca d'água** e **Abrir no navegador remoto**.
Atualize os sistemas operacionais que atingiram o Fim da Vida Útil	REC_024	Alta	VDA	Algumas máquinas estão executando sistemas operacionais (SO) que atingiram o Fim da Vida Útil. Isso representa riscos de segurança significativos e pode resultar na perda de suporte tanto da Citrix quanto do fornecedor do SO. Para manter um ambiente seguro e estável, certifique-se de que todos os

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				seus VDAs executem um sistema operacional compatível.
Atualize as versões do hypervisor que atingiram o Fim da Vida Útil	REC_025	Segurança	Hypervisor	Detalhes: Alguns hypervisors estão executando versões que atingiram o Fim da Vida Útil. Isso representa um risco para a estabilidade do ambiente e limita a capacidade da Citrix de fornecer suporte total. Para manter um ambiente seguro e compatível, atualize para uma versão de hypervisor suportada pelo fornecedor. Revise regularmente as notas de versão do fornecedor e a documentação de compatibilidade

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				para se manter alinhado com as melhores práticas e requisitos da plataforma.
Use HTTPS para conexões de host	REC_039	Médio	Geral	Algumas conexões de host estão atualmente configuradas com HTTP em vez de HTTPS. Para garantir a comunicação segura com seu hipervisor, atualize essas conexões para usar HTTPS. Isso requer a habilitação de HTTPS em seu hipervisor e a garantia de que certificados TLS válidos estejam em vigor.
Resolver vulnerabilidades de segurança do VDA	REC_040	Alta	VDA	Vulnerabilidades de segurança afetam algumas de suas versões de VDA. Revise o Boletim de Segurança da Citrix e aplique as correções ou

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				mitigações necessárias para garantir a integridade e conformidade do sistema.
Resolver vulnerabilidades de segurança do aplicativo Citrix Workspace	REC_041	Alta	Aplicativo Workspace	Vulnerabilidades de segurança afetam algumas versões do aplicativo Citrix Workspace em dispositivos de endpoint. Revise o Boletim de Segurança da Citrix e aplique as correções ou mitigações necessárias para garantir a integridade e conformidade do sistema.
Atualizar versões do servidor StoreFront que atingiram o Fim da Vida Útil	REC_043	Alta	StoreFront	Alguns servidores StoreFront estão executando versões que atingiram o Fim da Vida Útil e não são mais suportadas pela Citrix. Para manter um ambiente

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				seguro e suportável, atualize todos os servidores StoreFront afetados para a versão LTSR ou CR mais recente.
Use HTTPS para a URL base do StoreFront	REC_044	Alta	StoreFront	Algumas URLs base do StoreFront estão atualmente configuradas com HTTP em vez de HTTPS. Para proteger as credenciais do usuário e dados confidenciais, configure seus servidores StoreFront e balanceadores de carga associados para usar HTTPS. Certifique-se de que a URL base comece com 'https://'. Isso garante que todas as comunicações sejam criptografadas

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				e ajuda a prevenir ameaças de segurança, como ataques man-in-the-middle.
Use HTTPS para comunicação entre StoreFront e Cloud Connectors	REC_045	Alta	StoreFront	O tráfego entre StoreFront e Cloud Connectors está sendo transmitido atualmente por HTTP não criptografado, o que pode expor as credenciais do usuário a ameaças de segurança. Para proteger seu ambiente, habilite HTTPS nos Cloud Connectors e configure o StoreFront para usar conexões seguras.
Revise as lojas StoreFront com acesso anônimo habilitado	REC_052	Médio	StoreFront	O acesso anônimo está habilitado para algumas lojas StoreFront, permitindo que os usuários iniciem

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				aplicativos sem autenticação. Para mitigar potenciais riscos de segurança, revise essas lojas e remova as não utilizadas.

Nota:

As recomendações relacionadas ao StoreFront exigem configuração adicional. Consulte Configurar o StoreFront para verificação do Advisor para obter detalhes.

Recomendações de confiabilidade

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
Configurar agendamentos de reinício para grupos de entrega multissessão	REC_004	Alto	VDA	Alguns grupos de entrega de múltiplas sessões não têm agendamentos de reinício configurados. Reinícios agendados ajudam a manter o desempenho ideal, a estabilidade e a disponibilidade de recursos em

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				VDAs de SO de múltiplas sessões. Para garantir a continuidade do serviço e reduzir o tempo de inatividade, crie pelo menos dois agendamentos de reinício. Agende reinícios alternados com restrições de tags, marcando os VDAs em grupos, como 'Par' e 'Ímpar'.
Agendar reinícios alternados para grupos de entrega de múltiplas sessões	REC_005	Médio	VDA	Alguns grupos de entrega de múltiplas sessões têm apenas um agendamento de reinício configurado. Para garantir a continuidade do serviço e reduzir o tempo de inatividade, crie pelo menos dois agendamentos de reinício. Agende reinícios

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				alternados com restrições de tags, marcando os VDAs em grupos, como 'Par' e 'Ímpar'.
Hospedar aplicativos em vários VDAs	REC_006	Alto	VDA	Alguns aplicativos publicados são hospedados em apenas um VDA, o que pode afetar a continuidade do serviço e levar a riscos de tempo de inatividade. Garanta que cada aplicativo seja hospedado em vários VDAs em um grupo de entrega para ajudar a manter a disponibilidade e a confiabilidade.
Habilitar a continuidade do serviço para o Citrix Workspace	REC_007	Alto	Citrix Workspace	A continuidade do serviço não está habilitada, o que significa que, durante uma interrupção do serviço, os

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				usuários podem não conseguir iniciar sessões. Habilite a continuidade do serviço para melhorar a disponibilidade adicionando uma camada extra de resiliência que mantém o acesso do usuário final a aplicativos e desktops, apesar da saúde da rede ou do serviço.
Atualize os VDAs para corresponder ao nível funcional do catálogo	REC_008	Alta	VDA	Algumas máquinas usam uma versão anterior do VDA não suportada pelo nível funcional mínimo do catálogo, o que pode impedi-las de se registrar. Para evitar problemas de registro, atualize as versões anteriores do VDA para corresponder

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				ao nível funcional do catálogo.
Implante Cloud Connectors em suas zonas	REC_014	Alta	Cloud Connector	Menos de dois Cloud Connectors estão implantados em algumas de suas zonas (locais de recursos). Implante pelo menos dois Cloud Connectors por local de recurso para manter a disponibilidade e a resiliência durante as atualizações do Connector. Os locais de recursos devem seguir o modelo N + 1, onde N é o requisito de linha de base com base no tamanho da implantação e o 1 adicional fornece redundância.
Agende as atualizações do Connector	REC_015	Média	Cloud Connector	Algumas zonas (locais de recursos) não

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				têm um horário de início agendado para as atualizações do Connector. Para garantir que as atualizações ocorram apenas durante as janelas de manutenção planejadas e reduzir a interrupção do serviço, agende as atualizações do Connector para um horário e dia da semana preferenciais.
Coloque os Cloud Connectors no mesmo domínio	REC_028	Médio	Cloud Connector	Algumas zonas (locais de recursos) contêm Cloud Connectors unidos a domínios diferentes. Essa configuração pode levar a registros de VDA atrasados ou falhos, especialmente no modo Local Host Cache

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				(LHC). Para melhorar a confiabilidade e reduzir riscos, certifique-se de que todos os Cloud Connectors dentro de uma determinada zona pertençam ao mesmo domínio.
Habilite a comunicação entre Cloud Connectors para um desempenho LHC confiável	REC_029	Alto	Cloud Connector	Algumas zonas (locais de recursos) têm vários brokers de Local Host Cache (LHC) eleitos. Isso pode fazer com que os registros de VDA sejam divididos entre os Cloud Connectors no modo LHC, levando a falhas intermitentes de inicialização. Para evitar isso, certifique-se de que todos os Cloud Connectors em cada zona afetada possam

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				se comunicar entre si em http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection.
Verifique as configurações de resiliência	REC_030	Médio	Geral	As configurações de resiliência da sua implantação não foram verificadas recentemente. Manter as configurações de resiliência adequadas é fundamental para garantir acesso ininterrupto a aplicativos e desktops, especialmente durante interrupções inesperadas do serviço. Verifique suas configurações de resiliência regularmente para garantir que sua implantação

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				esteja configurada corretamente para manipular interrupções potenciais e proteger a produtividade do usuário.
Habilitar verificação de integridade avançada para lojas StoreFront	REC_036	Médio	StoreFront	Uma ou mais lojas em alguns servidores StoreFront não têm a verificação de integridade avançada habilitada. O StoreFront usa as informações adicionais dos resultados da verificação de integridade avançada para garantir que as solicitações de inicialização sejam enviadas para o local de recurso (zona) apropriado no modo Local Host Cache (LHC). Sem a verificação de integridade avançada, as inicializações

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				podem falhar no modo LHC. Para melhorar a resiliência do seu ambiente Citrix, habilite a verificação de integridade avançada para todas as lojas nos servidores StoreFront.
Adicionar todos os Cloud Connectors como servidores STA no StoreFront e NetScaler Gateway	REC_037	Médio	Cloud Connector	Alguns Cloud Connectors não estão configurados como servidores Secure Ticket Authority (STA), o que os impede de receber solicitações STA do StoreFront. Para evitar falhas de inicialização no modo Local Host Cache, certifique-se de que todos os Cloud Connectors sejam adicionados como servidores STA

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				tanto no StoreFront quanto no NetScaler Gateway.
Garantir redundância do servidor StoreFront	REC_042	Alta	StoreFront	Alguns grupos de servidores StoreFront contêm apenas um servidor, criando um único ponto de falha e uma falta de redundância em caso de interrupção. Para melhor resiliência, implante pelo menos dois servidores StoreFront em um grupo de servidores e coloque-os atrás de um balanceador de carga para garantir failover contínuo e acesso ininterrupto.
Verificar a comunicação do Cloud Connector	REC_047	Médio	StoreFront	Alguns locais de recursos (zonas) contêm Cloud Connectors que

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
com o StoreFront				não estão recebendo solicitações do StoreFront para enumeração de recursos. Esse problema pode ocorrer se os Cloud Connectors não estiverem listados no StoreFront ou se houver um problema de comunicação, como um certificado expirado no Cloud Connector. Certifique-se de que todos os Cloud Connectors estejam listados no StoreFront e estejam acessíveis. Se você não estiver usando uma implantação local do StoreFront, ignore esta recomendação.

Observação:

As recomendações relacionadas ao StoreFront exigem configuração adicional. Consulte Configurar o StoreFront para verificação do Advisor para obter detalhes.

Recomendações de desempenho

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
Otimizar Cloud Connectors para o modo LHC	REC_019	Alta	Cloud Connector	Alguns Cloud Connectors têm menos de quatro núcleos de CPU por soquete, o que pode afetar a capacidade dos usuários de enumerar e iniciar recursos disponíveis enquanto estiverem no modo LHC. Para maximizar a disponibilidade de recursos para LHC e evitar gargalos de desempenho, configure as máquinas Cloud Connector para ter pelo menos quatro núcleos por soquete.

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
Aprimorar o hardware do Cloud Connector	REC_020	Alta	Cloud Connector	O alto uso de CPU, memória ou disco pode afetar o desempenho e a disponibilidade do Cloud Connector. Para evitar a degradação do desempenho e manter a confiabilidade, aumente a CPU, a memória ou o armazenamento para os Cloud Connectors.
Dimensionar corretamente máquinas com alto consumo de recursos	REC_023	Média	VDA	Algumas máquinas mostram sinais de sobrecarga de desempenho, como alta utilização de CPU ou memória, ou uma alta contagem de sessões. Isso indica que as máquinas estão subdimensionadas para manipular as cargas de

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				trabalho que suportam, o que pode levar a uma experiência de usuário ruim e desempenho reduzido. Considere alterar o tamanho da máquina para aumentar os recursos alocados para a máquina ou realocar usuários avançados para um grupo de entrega que tenha máquinas de alto desempenho.
Reduza o número de conexões de host em suas zonas	REC_026	Alta	Geral	O número de conexões de host em algumas zonas (locais de recurso) excede o limite recomendado, o que pode resultar em degradação do desempenho. Reduza o número de conexões de

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				host nas zonas para não mais do que o limite recomendado.
Reduza o número de VDAs em suas zonas	REC_027	Alta	VDA	O número de VDAs em algumas zonas (local de recurso) excede o limite recomendado, aumentando o risco de falhas nos registros de VDA e degradação do balanceamento de sessão, especialmente no modo Local Host Cache (LHC). Para mitigar esses riscos, redistribua os VDAs movendo alguns para outras zonas. Certifique-se de que seu método para configurar o registro de VDA seja atualizado de acordo.
Avalie a alocação de recursos para	REC_031	Média	Provisionamento	Alguns servidores Citrix

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
servidores PVS				Provisioning (PVS) mostram sinais de sobrecarga de desempenho, como alta utilização de CPU ou memória. A alocação insuficiente de recursos do servidor pode resultar em baixo desempenho e tempos de inicialização estendidos. Considere aumentar a alocação de CPU e memória para esses servidores PVS conforme necessário.
Aumentar a alocação de recursos para servidores PVS	REC_032	Alta	Provisionamento	Alguns servidores Citrix Provisioning (PVS) mostram sinais de sobrecarga de desempenho, como utilização crítica de CPU ou memória. A alocação

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				insuficiente de recursos do servidor pode resultar em baixo desempenho e tempos de inicialização estendidos. Considere aumentar a alocação de CPU e memória para esses servidores PVS conforme necessário.
Avaliar o tamanho do disco de cache de gravação para dispositivos de destino PVS	REC_033	Média	VDA	O uso do disco de cache de gravação em alguns dispositivos de destino Citrix Provisioning (PVS) está se aproximando do limite. Para evitar problemas de desempenho e falhas de sessão do usuário, avalie o tamanho atual do disco de cache de gravação e aumente-o

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				conforme necessário.
Otimizar a configuração de GPO para VDAs	REC_035	Média	VDA	Algumas sessões de usuário experimentaram processamento prolongado de GPO durante o logon, impactando o desempenho. Para aumentar o controle sobre as configurações do ambiente, bloqueie a herança de Política de Grupo para suas unidades organizacionais de VDA e aplique apenas políticas e configurações de segurança relevantes. Além disso, considere aproveitar o Citrix Workspace Environment Management para processar as

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				configurações de forma assíncrona para logons de sessão mais rápidos.
Ativar pool de sockets para lojas StoreFront	REC_046	Médio	StoreFront	Algumas lojas StoreFront não têm o pool de sockets ativado. O pool de sockets aumenta a eficiência ao manter um pool de conexões de rede (sockets) prontamente disponíveis para comunicação com Delivery Controllers ou Cloud Connectors. Em vez de criar um novo socket para cada solicitação e depois fechá-lo (um processo de alto custo), o StoreFront reutiliza uma conexão existente do pool. Para melhorar o desempenho e

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				a eficiência geral do ambiente, ative o pool de sockets em todas as lojas, particularmente para conexões Transport Layer Security (TLS).
Coloque os servidores StoreFront em uma rede de baixa latência	REC_051	Médio	StoreFront	Foi detectada alta latência entre servidores em alguns grupos de servidores, o que pode levar a problemas de desempenho. A latência entre servidores em um grupo deve ser inferior a 40 ms (com assinaturas desativadas) ou 3 ms (com assinaturas ativadas). Coloque os servidores em uma rede de baixa latência ou separe-os em diferentes grupos de servidores.

Nota:

As recomendações relacionadas ao StoreFront exigem configuração adicional. Consulte Configurar o StoreFront para verificação do Advisor para obter detalhes.

Recomendações de excelência operacional

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
Atualizar VDAs para a versão mais recente	REC_002	Baixo	VDA	Algumas máquinas estão usando versões mais antigas do VDA. Atualize para a versão LTSR ou CR VDA mais recente para acessar novos recursos, melhorias e aprimoramentos de segurança.
Usar a tecnologia de provisionamento da Citrix	REC_003	Médio	Provisionamento	Todas as máquinas no site são provisionadas manualmente e não usam tecnologias de provisionamento da Citrix, como Machine Creation Services (MCS) ou Citrix Provisioning Services (PVS). Use MCS ou

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				PVS para garantir a consistência do VDA, minimizar tarefas manuais e otimizar as operações de dimensionamento do ambiente.
Nível funcional baixo	REC_009	Baixo	VDA	Alguns catálogos de máquinas têm um nível funcional inferior à versão VDA detectada, limitando o acesso a novos recursos em versões VDA posteriores. Para acessar esses recursos, altere o nível funcional para a versão mais recente suportada por todas as máquinas no catálogo.
Faça backup da configuração do seu site	REC_011	Alto	Geral	Você não tem um backup da configuração do seu site. Crie backups sob demanda ou

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				agendados para garantir que você tenha uma cópia pronta para uso das suas configurações Citrix para uma recuperação rápida.
Crie um novo backup da configuração do seu site	REC_012	Alto	Geral	Seu último backup da configuração do site foi há mais de três meses. Crie regularmente backups sob demanda ou agendados para manter uma cópia atualizada das suas configurações Citrix pronta para uma recuperação rápida.
Simplifique a configuração do catálogo com um perfil de máquina	REC_038	Baixo	Provisionamento	Alguns catálogos de máquinas se beneficiariam do uso de um perfil de máquina. Com um perfil de máquina, o

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				Machine Creation Services (MCS) captura as propriedades de hardware e os recursos específicos do hipervisor do perfil e provisiona eficientemente novas máquinas virtuais (VMs) no catálogo com a mesma configuração.
Redefinir contas do Active Directory corrompidas	REC_049	Médio	Provisionamento	Alguns catálogos de máquinas contêm contas AD marcadas como 'corrompidas' no Serviço de Identidade AD. Essas contas devem ser redefinidas para estarem disponíveis para operações de provisionamento subsequentes.

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
Substituir ponto de beacon obsoleto para StoreFront	REC_050	Médio	StoreFront	O aplicativo Citrix Workspace usa pontos de beacon configurados no StoreFront para determinar se os usuários estão conectados a redes internas ou externas. Você está usando ping.citrix.com como um beacon, que foi descontinuado e não está mais acessível. Substitua-o por uma URL acessível e pública no console de gerenciamento do StoreFront.
Desabilitar URL de Serviços XenApp para lojas StoreFront	REC_053	Alta	StoreFront	A URL dos Serviços XenApp (também conhecida como PNAgent) está habilitada para algumas lojas StoreFront. Este recurso

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				está obsoleto. Para compatibilidade e segurança, configure o aplicativo Citrix Workspace para se conectar ao StoreFront usando a URL da Loja e desabilite os Serviços XenApp no servidor. Se você tiver dispositivos legados que exigem PNAgent, ignore esta recomendação.
Descontinuar sites StoreFront não suportados	REC_054	Alta	StoreFront	Algumas lojas StoreFront estão vinculadas a tipos de sites não suportados. Migre os recursos para sites suportados e descontinue os sites não suportados.

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
Desabilitar a delegação Kerberos para lojas StoreFront	REC_055	Baixa	StoreFront	A delegação Kerberos está habilitada para algumas lojas StoreFront. A delegação Kerberos está obsoleta e só pode ser usada com o XenApp 6.5 e versões anteriores. Desabilite a delegação Kerberos para essas lojas StoreFront.
Revisar máquinas em modo de manutenção por períodos prolongados	REC_056	Médio	VDA	Algumas máquinas estão em modo de manutenção há mais de 14 dias. Revise as máquinas para determinar se devem ser retornadas ao serviço, desativadas ou mantidas em modo de manutenção com justificativa.
Reduza o tempo de solução de problemas	REC_058	Médio	Geral	Adicione um servidor de log para transferir com segurança

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
com o Always On Tracing				seus logs do Always On Tracing (AOT) para um servidor de log centralizado. Os logs são coletados em tempo real e estão disponíveis no Monitor, ajudando você a resolver problemas mais rapidamente e a otimizar as investigações de suporte.

Nota:

As recomendações relacionadas ao StoreFront exigem configuração adicional. Consulte Configurar o StoreFront para verificação do Advisor para obter detalhes.

Recomendações de otimização de custos

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
Habilitar o Autoscale para seus grupos de entrega	REC_010	Médio	VDA	Alguns grupos de entrega elegíveis não estão usando o Autoscale. Habilite o Autoscale para um

RECOMENDAÇÃO	ID	IMPACTO	COMPONENTE	DESCRIÇÃO
				gerenciamento consistente de energia da máquina, mantendo a disponibilidade enquanto equilibra efetivamente os custos e a experiência do usuário.
Liberar recursos não utilizados	REC_013	Médio	Geral	Algumas cargas de trabalho dedicadas, como máquinas ou aplicativos, não foram usadas por mais de 30 dias. Para reduzir gastos desnecessários e otimizar custos, libere máquinas não utilizadas de volta para o pool disponível e gerencie aplicativos não utilizados.

Serviço de Atualização de VDA (VUS)

O Serviço de Atualização de VDA (VUS) da Citrix é um componente do Citrix Desktop as a Service (DaaS) que facilita um processo de atualização simplificado para Virtual Delivery Agents (VDAs) persistentes dentro do seu ambiente Citrix. O serviço ajuda a manter seus ambientes atualizados com as versões mais recentes do VDA, melhorando o desempenho e a segurança, e habilitando novos recursos do Citrix DaaS™.

> **Nota:**

> Antes de agendar uma atualização, o Serviço de Atualização de VDA verifica se o sistema operacional atual de cada VDA é compatível com a versão de destino selecionada. Se um VDA executa um sistema operacional que a versão de destino não suporta mais, esse destino não é oferecido para o VDA, e o VDA é relatado como Atualizado.

> Os administradores podem usar o VUS para verificar atualizações, agendar atualizações e monitorar o progresso da atualização. As atualizações podem ser iniciadas imediatamente ou agendadas para uma data e hora específicas, permitindo que você escolha o melhor momento para suas atualizações.

Atualizar VDAs nunca foi tão fácil. Instale o Agente de Atualização de VDA em seus VDAs ou imagens, clique com o botão direito na máquina ou catálogo de máquinas na interface de configuração completa, selecione “Atualizar VDAs” e selecione as opções que melhor se adequam ao seu ambiente.

Antes de atualizar, revise as opções do ciclo de atualização. Duas trilhas de atualização estão disponíveis para seus VDAs: Long-Term Service Release (LTSR) e Current Release (CR). O LTSR tem um ciclo de vida de suporte mais longo, proporcionando mais estabilidade e atualizações menos frequentes. As versões CR são lançadas com mais frequência, fornecendo os recursos mais recentes e melhores. Para obter mais informações, consulte Marcos do Ciclo de Vida.

Pré-requisitos para atualizar VDAs usando VUS

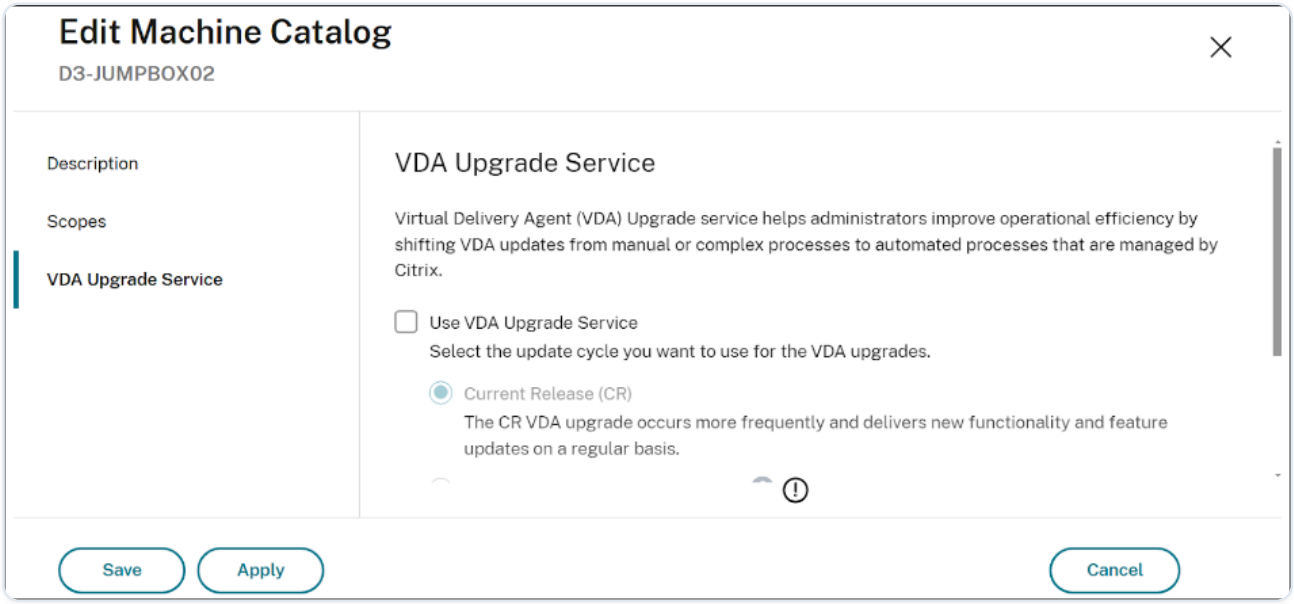
Para realizar atualizações de VDA usando VUS, os seguintes pré-requisitos devem ser atendidos.

Habilitar o Serviço de Atualização de VDA

Para habilitar o recurso Serviço de Atualização de VDA, use a opção Atualização de VDA ao criar ou editar um Catálogo de Máquinas. Os administradores devem escolher um dos seguintes ciclos de atualização ao habilitar o VUS:

- LTSR
- CR
- LTSR Versão de Acesso Antecipado (EAR)
- CR EAR

Para habilitar o Serviço de Atualização de VDA para um catálogo de máquinas a partir da interface de configuração completa do DaaS, clique com o botão direito do mouse em um catálogo, clique em “Editar Catálogo”, selecione a guia “Serviço de Atualização de VDA”, marque a caixa “Usar Serviço de Atualização de VDA” e selecione uma trilha de atualização.



Para habilitar o Serviço de Atualização de VDA para um catálogo de máquinas usando PowerShell, use o cmdlet `Set-VusCatalogUpgradeType`.

O tipo de atualização pode ser definido como “LTSR”, “CR”, “EAR_CR” ou “EAR_LTSR”.

Exemplo: `Set-VusCatalogUpgradeType -CatalogName "Workstation catalog" -UpgradeType LTSR`

> **Nota:**

> Habilitar a opção de Atualização de VDA não resultará na atualização automática de VDAs. Todas as atualizações de VDA através do VUS devem ser iniciadas como uma tarefa separada, explicitamente realizada pelos administradores.

Requisitos do VDA

Versão do VDA

2109 CR ou posterior, ou 2203 LTSR ou posterior

Sistema operacional do VDA de origem

O Serviço de Atualização do VDA oferece apenas uma versão de destino cujos requisitos de sistema incluem o sistema operacional atual do VDA. Se um VDA executa um sistema operacional que foi removido do suporte na versão de destino — por exemplo, Windows Server 2016, que não é suportado como um SO de VDA a partir do CVAD 2407 em diante — esse destino não é oferecido, e o VDA é relatado como Atualizado sem nenhuma atualização disponível. Para atualizar tal VDA, re-image-o para um sistema operacional suportado. Para os sistemas operacionais que cada versão suporta, consulte os Requisitos de sistema para essa versão e CTX224843.

Tipo de Provisionamento

- Máquinas persistentes de sessão única ou multi-sessão provisionadas usando serviços ou tecnologias de provisionamento que não são da Citrix™.
- Máquinas persistentes provisionadas por MCS de sessão única (ingressadas no AD, ingressadas no Microsoft Entra e não ingressadas no domínio).
- Máquinas de Acesso Remoto para PC.
- Citrix HDX™ Plus para Windows 365.

Agente de Atualização do VDA

- O Agente de Atualização do VDA deve estar instalado e ativo no VDA. O agente pode ser instalado:
  - Como um componente adicional, ao atualizar seu VDA ou modificar a instalação do VDA.
  - Usando o MSI autônomo que está disponível na ISO do Citrix Virtual Apps and Desktops™.
    - Nome do MSI: CitrixUpgradeAgent_x64.msi
    - Caminho: x64\Virtual Desktop Components

- Para atualizar VDAs LTSR para versões CU LTSR, o Agente de Atualização do VDA deve ser a versão 7.36.0.7 ou posterior.

> **Nota:**
>
> O agente de atualização do VDA é atualizado automaticamente se o VDA tiver acesso aos URLs listados em Conectividade.

Permissões

Você deve ter a função de Administrador Completo ou Administrador de Catálogo de Máquinas no Citrix DaaS.

Estado do VDA

Para que as atualizações agendadas via VUS prossigam conforme o esperado, os VDAs destinados à atualização devem atender aos seguintes pré-requisitos:

- O VDA não deve ser colocado manualmente em modo de manutenção.
- Para que uma atualização do VDA ocorra com sucesso, nenhum usuário pode estar logado.
  - Os VDAs são colocados em modo de manutenção quando o processo de atualização começa a drenar as sessões de usuário durante toda a janela de atualização. Eles são removidos do modo de manutenção assim que a atualização é concluída com sucesso.
  - Se um usuário tiver uma sessão ativa ou desconectada durante toda a duração da janela de atualização, a atualização será cancelada ao final da Janela de Atualização.

> **Nota:**
>
> Sessões ativas e desconectadas podem ser encerradas usando a opção de logoff forçado no VUS.

  - VDAs não provisionados via MCS (provisionados manualmente) devem ser adicionados a um Grupo de Entrega antes de realizar uma atualização via VUS.
  - Os VDAs devem estar ligados.

> **Nota:**

> O AutoScale™ não para de gerenciar a energia das máquinas quando as atualizações do VDA são agendadas. Considere desabilitar os agendamentos do AutoScale no Grupo de Entrega quando as atualizações estiverem em andamento.

Conectividade

- Os VDAs devem ser capazes de se comunicar com os seguintes URLs:
  - Se estiver usando a rede de entrega de conteúdo (CDN) da Citrix para baixar o instalador do VDA, os VDAs devem ser capazes de se comunicar com os seguintes URLs.
    - Produção - Gov: `<https://prod-us-gov-vus-release-endpoint-*.z01.azurefd.us/prod-us-gov-vus-release-container/*>`
    - Produção - Estados Unidos (EUA): `<https://prod-us-vus-storage-endpoint.azureedge.net/*>`
    - Produção - União Europeia (UE): `<https://prod-eu-vus-storage-endpoint.azureedge.net/*>`
    - Produção - Ásia-Pacífico Sul (APS): `<https://prod-aps-vus-storage-endpoint.azureedge.net/*>`
    - Produção - Japão (JP): `<https://prod-jp-vus-storage-endpoint.azureedge.net/*>`
  - Para verificar se o instalador do VDA é assinado por um certificado válido, os VDAs devem se comunicar com os seguintes URLs. Aplicável também à Produção Gov, sem alterações.
    - `<http://crl3.digicert.com/>` *
    - `<http://crl4.digicert.com/>` *
    - `<http://ocsp.digicert.com/>` *
    - `<http://cacerts.digicert.com/>` *
  - O Agente de Atualização do VDA se comunica com o DaaS nos seguintes URLs.
    - Governo de Produção https://.xendesktop.us/citrix/vdaupdateservice/*
    - https://.xendesktop.net/citrix/VdaUpdateService/*, onde é o parâmetro de ID do cliente exibido na guia Clientes Seguros (Gerenciamento de Identidade e Acesso > Acesso à API > Clientes Seguros) do console de gerenciamento do Citrix Cloud.

VDAs com configurações de proxy

- Compatível com o Agente de Atualização do VDA versão 7.40 e superior.
- Apenas proxies no formato Hostname: Porta (IP:Porta) e arquivo PAC são suportados. Proxies SOCKS5 não são suportados.
- O Agente de Atualização do VDA deve ser configurado para usar um proxy usando a interface de configuração completa ou o registro.
    - Configuração de proxy do Agente de Atualização do VDA usando a interface de configuração completa
        - Habilite a configuração de Política Citrix de proxy de atualização do VDA para os VDAs que usam um proxy.
        - Insira o endereço do proxy ou o caminho para o arquivo PAC nas configurações.
    - Configuração de proxy do Agente de Atualização do VDA usando o registro
        - Chave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
            - Tipo de valor: String
            - Nome do valor: ProxySettings
            - Dados do valor: Endereço do proxy ou caminho para o arquivo pac.
            - Por exemplo:
                - Endereço do proxy: http://<URL or IP>:\<port>
                - Arquivo Pac: http://<URL or IP>/\<path/\<filename>.pac
- A validação de certificado usa a CryptoAPI do Windows, que não oferece suporte à comunicação por proxy.
    - Para configurar o proxy do sistema no VDA para facilitar chamadas CRL de saída. Insira um dos seguintes comandos na linha de comando do VDA para configurar o proxy do sistema:
        - Para copiar as configurações de proxy do Internet Explorer:
            - netsh winhttp import proxy source=ie
        - Para utilizar uma configuração de proxy separada:
            - netsh winhttp set proxy proxy-server=http://Proxy_Server:Port

VDAs instalados usando o VDAWorkstationCoreSetup.exe

Se o VDA foi originalmente instalado usando `VDAWorkstationCoreSetup.exe`, ele ainda pode ser atualizado usando o VUS, que utiliza VDAWorkstationSetup.exe. Ao atualizar VDAs que foram instalados com `VDAWorkstationCoreSetup.exe` usando o VUS, você deve revisar as opções de instalação para garantir que apenas os recursos desejados estejam habilitados, especialmente se estiver migrando de uma instalação principal mínima.

Pré-requisitos da Nuvem Governamental para atualizações de VDA (VUS)

Este artigo documenta os pré-requisitos do lado do cliente para atualizar VDAs através do Serviço de Atualização de VDA (VUS) no ambiente de Produção Governamental.

Use esta orientação quando os controles de firewall de saída ou proxy forem impostos e a saída for restrita.

Pré-requisitos

Esses pré-requisitos se aplicam a clientes governamentais que usam o VUS para atualizar VDAs persistentes e precisam permitir as conexões de saída necessárias para download de pacotes, recuperação de agendamento e relatório de versão.

Esta orientação é adicional aos pré-requisitos padrão do VUS em Pré-requisitos para atualizar VDAs usando VUS.

Acesso de endpoint de saída necessário

Permitir HTTPS de saída (TCP 443) das seguintes fontes:

- VDAs que executam o Agente de Atualização de VDA.
- Cloud Connectors, quando o tráfego é roteado pelo conector.

Permitir os seguintes padrões de destino:

- Padrão de endpoint CDN de lançamento do VUS do Governo de Produção: `<https://prod-us-gov-vus-release-endpoint->` *.z01.azurefd.us/prod-us-gov-vus-release-container/*
- Padrão de endpoint REST DDC Governamental por cliente: https://.xendesktop.us/citrix/vdaupdateservice/*

Por que esses endpoints são necessários

PADRÃO DE ENDPOINT	FINALIDADE	USADO POR
`<https://prod-us-gov-vus-release-endpoint->`*.z01.azurefd.us/prod-us-gov-vus-release-container/*	Baixa pacotes de instalação do VDA para atualizações agendadas.	Fluxo de download do Agente de Atualização do VDA
https://[customerId].xendesktop.us/citrix/vdaupdateservice/*	Obtém agendamentos do VUS e publica chamadas de relatório de versão do VDA.	Chamadas do plano de controle do Agente de Atualização do VDA

Se qualquer um dos endpoints for bloqueado por firewall, proxy, política de inspeção SSL ou filtragem de DNS, as atualizações poderão falhar.

Pré-requisitos de armazenamento governamental e KeyVault

A conta de armazenamento governamental e os recursos do KeyVault usados pelo pipeline de lançamento do VUS são gerenciados no lado do serviço.

A ação do cliente é tipicamente limitada à configuração da política de saída de rede para VDAs e Cloud Connectors. Se sua organização aplicar controles de saída adicionais ou restrições de roteamento privado, coordene a validação com suas equipes de suporte e segurança da Citrix antes de agendar atualizações de produção.

Considerações sobre o limite FedRAMP

- Revise seus controles de limite FedRAMP para HTTPS de saída para endpoints do Azure Government Front Door (*.azurefd.us) e endpoints xendesktop.us específicos do cliente.
- Documente os padrões de destino aprovados e a lógica de controle em seu SSP e registros de alteração.
- Se a inspeção TLS for obrigatória, valide que o tratamento de certificados não interrompa o download do instalador VDA ou a API comunicação.

Lista de verificação de pré-atualização

- Confirme a resolução DNS e a acessibilidade TCP 443 de cada sub-rede VDA para o endpoint *.azurefd.us necessário.
- Confirme a resolução DNS e a acessibilidade TCP 443 de cada sub-rede VDA para https://.xendesktop.us.

- Confirme a mesma acessibilidade dos Cloud Connectors para caminhos de tráfego roteados por conector.
- Execute uma atualização piloto do VUS em um pequeno conjunto de máquinas e verifique o download do pacote e o sucesso do relatório de versão.

Atualizar VDAs usando VUS

Você pode iniciar atualizações de VDA através do serviço de atualização de VDA selecionando o catálogo de máquinas de destino, máquina individual ou grupo de máquinas e, em seguida, selecionando “Atualizar VDAs”.

> **Nota:**

> A Citrix® recomenda fazer backup dos VDAs antes de realizar as atualizações, sempre que possível.

Agendamento de Atualizações

O processo de atualização de VDA na Citrix pode ser realizado no nível do catálogo, no nível do grupo de máquinas ou no nível da máquina individual, dependendo dos requisitos. As atualizações podem ser configuradas para iniciar imediatamente ou podem ser agendadas para uma data e hora com até 7 dias de antecedência.

Considerações

- **Escopo de Catálogo vs. Grupo de Máquinas vs. Máquina:** As atualizações de catálogo são ideais para atualizações em massa, enquanto a atualização de máquinas individualmente ou por grupos permite um controle mais granular.
- **Agendamento:** As atualizações podem ser agendadas com até 7 dias de antecedência. Se estiver usando atualizações no nível do catálogo de máquinas, as máquinas adicionadas ao catálogo após o agendamento da atualização não são incluídas como parte da atualização agendada existente.

Restringir atualizações a máquinas marcadas

No nível do catálogo de máquinas, agora você pode limitar as atualizações de VDA apenas às máquinas que possuem uma tag de máquina selecionada.

No Web Studio, ao iniciar uma atualização no nível do catálogo, escolha **Atualizar máquinas que correspondem à tag** em vez de **Atualizar todas as máquinas**. Em seguida, selecione uma tag no seletor de tags.

Apenas as máquinas nesse catálogo com a tag selecionada são incluídas no escopo da atualização.

Esta opção suporta ambas as trilhas de atualização CR e LTSR.

Use esta opção para estratégias de implantação baseadas em anéis quando você deseja validar uma versão mais recente do VDA em um subconjunto piloto antes de agendar atualizações para o catálogo completo.

Escopo

- Disponível apenas para atualizações em nível de catálogo.
- Não disponível para atualizações em nível de grupo de entrega.
- Não disponível para atualizações em nível de máquina individual.

Comportamento da UI

Ao selecionar **Atualizar máquinas que correspondem à tag**:

- Um seletor de tags aparece e mostra as tags presentes no catálogo selecionado.
- A contagem de máquinas na página **Agendar** reflete apenas as máquinas marcadas com tags no escopo.
- A contagem de máquinas na página **Resumo** reflete apenas as máquinas marcadas com tags no escopo.

Principais Diferenças

RECURSO	ATUALIZAÇÃO POR CATÁLOGO	ATUALIZAÇÃO POR MÁQUINA	GRUPO DE MÁQUINAS
Escopo das atualizações	Catálogo inteiro	Máquina individual	Grupo de máquinas de um Catálogo de Máquinas
Controle de agendamento	Um único agendamento se aplica a todos os VDAs no catálogo de máquinas, ideal para	Os VDAs são agendados individualmente, o que é usado principalmente para	Os VDAs são agendados em grupos, oferecendo a flexibilidade de atualizar diferentes

RECURSO	ATUALIZAÇÃO POR CATÁLOGO	ATUALIZAÇÃO POR MÁQUINA	GRUPO DE MÁQUINAS
	operações de atualização em larga escala	testes e atualizações pontuais	grupos de VDAs em momentos diferentes
Gerenciamento	Gerenciado através do nó de catálogos de máquinas na interface de Configuração Completa ou do cmdlet `New-VusCatalogSchedule`	Gerenciado através do nó de Pesquisa na interface de Configuração Completa ou do cmdlet `New-VusMachineUpgrade`	Gerenciado através do nó de Pesquisa na interface de Configuração Completa, ou passando uma lista de máquinas para o cmdlet `New-VusMachineUpgrade`
Caso de Uso	Atualizações em massa para um Catálogo de Máquinas inteiro	Controle granular para atualizações direcionadas e cenários de teste	Controle direcionado de um subconjunto de VDAs. Pode ser usado para escalonar as atualizações dentro de um catálogo
Versões de VDA disponíveis	Para CR e todas as versões de VDA LTSR atualmente suportadas, a versão mais recente, bem como as 2 versões anteriores (N-2), estão disponíveis para atualização. Consulte Versões de VDA disponíveis para obter mais informações	Para CR e todas as versões de VDA LTSR atualmente suportadas, a versão mais recente, bem como as 2 versões anteriores (N-2), estão disponíveis para atualização. Consulte Versões de VDA disponíveis para obter mais informações	Apenas a versão mais recente do VDA LTSR ou CR está disponível para ser atualizada
Componentes Adicionais	Instala ou atualiza componentes VDA em cada VDA. Deixar um	Instala ou atualiza o componente VDA no VDA. Deixar um componente	Componentes adicionais não podem ser gerenciados pelo

RECURSO	ATUALIZAÇÃO POR CATÁLOGO	ATUALIZAÇÃO POR MÁQUINA	GRUPO DE MÁQUINAS
	componente desmarcado não desinstalará o recurso, mas o componente não será atualizado	desmarcado não desinstalará o recurso, mas o componente não será atualizado	serviço de atualização do VDA ao atualizar um grupo de máquinas. Nota: Recursos adicionais, como “Habilitar Limpeza de Restauração”, estão disponíveis para atualizações de grupos de máquinas
Recursos Adicionais	Recursos adicionais podem ser habilitados ou atualizados	Recursos adicionais podem ser habilitados ou atualizados	Recursos adicionais podem ser habilitados ou atualizados
Simultaneidade	Controlado como uma configuração ao agendar a atualização. Consulte Simultaneidade para obter mais informações	Um único VDA é atualizado	Automaticamente balanceado por carga com base no número de VDAs selecionados como parte do agendamento de atualização
Limite de Falha	Um limite de falha pode ser definido para evitar futuras atualizações se um número fornecido de VDAs falhar nas atualizações. Consulte Limite de Falha para obter mais informações.	Os limites de falha não são aplicáveis para uma atualização por máquina	Os limites de falha não estão disponíveis para atualizações de grupo de máquinas. Considere definir o tamanho do grupo de máquinas a ser atualizado como o número máximo de VDAs que seria uma quantidade de falha aceitável

Como funcionam as atualizações agendadas

O Agente de Atualização do VDA nos VDAs se comunica com o Citrix Cloud™ periodicamente para determinar se o VDA deve ser atualizado. Os VDAs podem ser agendados para atualização imediata ou com até 7 dias de antecedência. Ao agendar uma atualização com antecedência, você pode definir a data e a hora (em UTC) em que a atualização começa.

A duração da atualização define o período de tempo após a hora de início da atualização agendada durante o qual as atualizações ocorrem. Por padrão, para atualizações de catálogo de máquinas e grupos de máquinas, a Citrix balanceia a carga das atualizações de VDA durante toda a duração da atualização para melhorar o desempenho e evitar gargalos.

Assim que uma atualização começa, o VDA é colocado em modo de manutenção até que a atualização seja concluída. Se houver uma sessão presente no VDA, o VDA não será atualizado até que não haja sessões presentes. Nenhuma nova sessão pode ser intermediada para o VDA quando ele está em modo de manutenção. Se um usuário se desconectar de uma sessão durante uma janela de atualização, o usuário não poderá se reconectar até que a atualização seja concluída.

O VDA continuará a tentar uma atualização até que a duração da atualização agendada seja concluída. Se uma sessão estiver presente durante toda a duração da atualização, a atualização será cancelada e o modo de manutenção será desativado para o VDA. Considere uma duração de atualização mais longa para melhorar a taxa de sucesso da atualização do VDA.

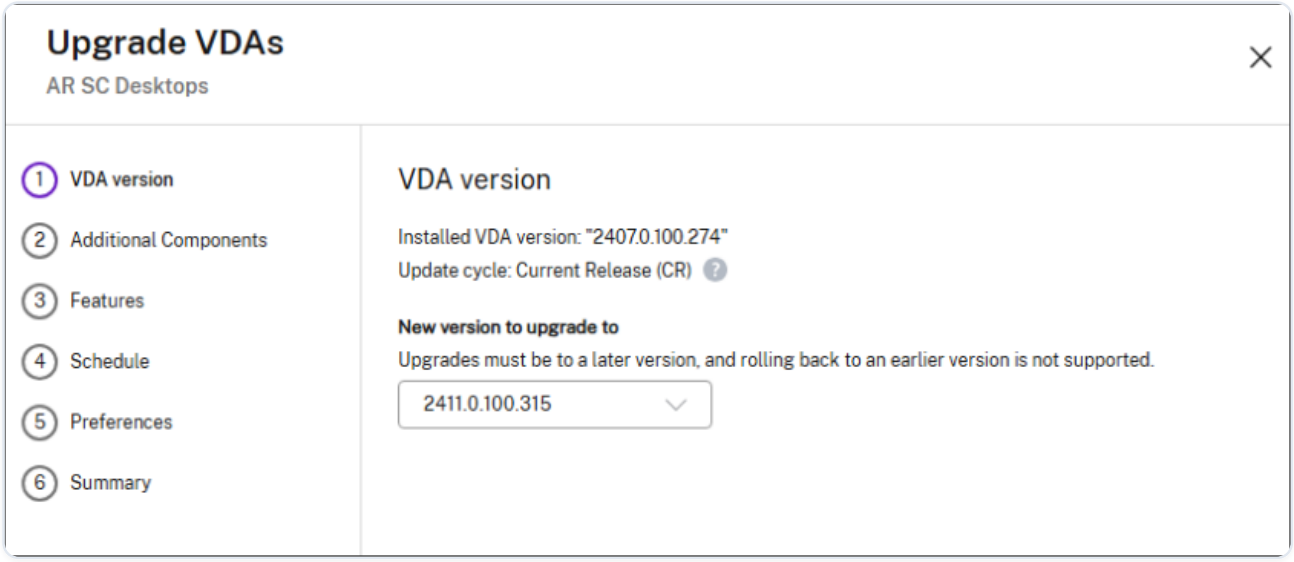
> **Nota:**
>
> VDAs colocados manualmente em modo de manutenção antes de uma atualização agendada falharão na atualização.

Versões de VDA Disponíveis

Novas versões de VDA estão disponíveis para atualização por meio do serviço de atualização de VDA logo após as novas versões de VDA serem disponibilizadas ao público. O serviço de atualização de VDA mantém N-2 versões do VDA para versões CR e N-2 versões CU para todas as versões LTSR que são atualmente suportadas.

O assistente de Atualização de VDAs lista apenas as versões de destino compatíveis com o sistema operacional atual de cada VDA selecionado. Um destino que removeu o suporte para o sistema operacional de um VDA não é mostrado para esse VDA.

Na interface de configuração completa, ao atualizar um catálogo ou uma máquina individual, a interface do usuário solicita a versão para a qual você deseja atualizar seus VDAs.



Para determinar as versões de VDA disponíveis usando o PowerShell, use o cmdlet `Get-VusAvailableVdaVersion`.

Sem passar uma máquina ou um catálogo com o cmdlet, o cmdlet retornará a versão mais recente disponível para todos os caminhos de atualização.

Para obter as versões específicas disponíveis para um recurso, passe um VDA (-MachineName, -MachineUid ou -MachineUuid) ou catálogo (-CatalogName, -CatalogUid ou -CatalogUuid) com o cmdlet `Get-VusAvailableVdaVersion`.

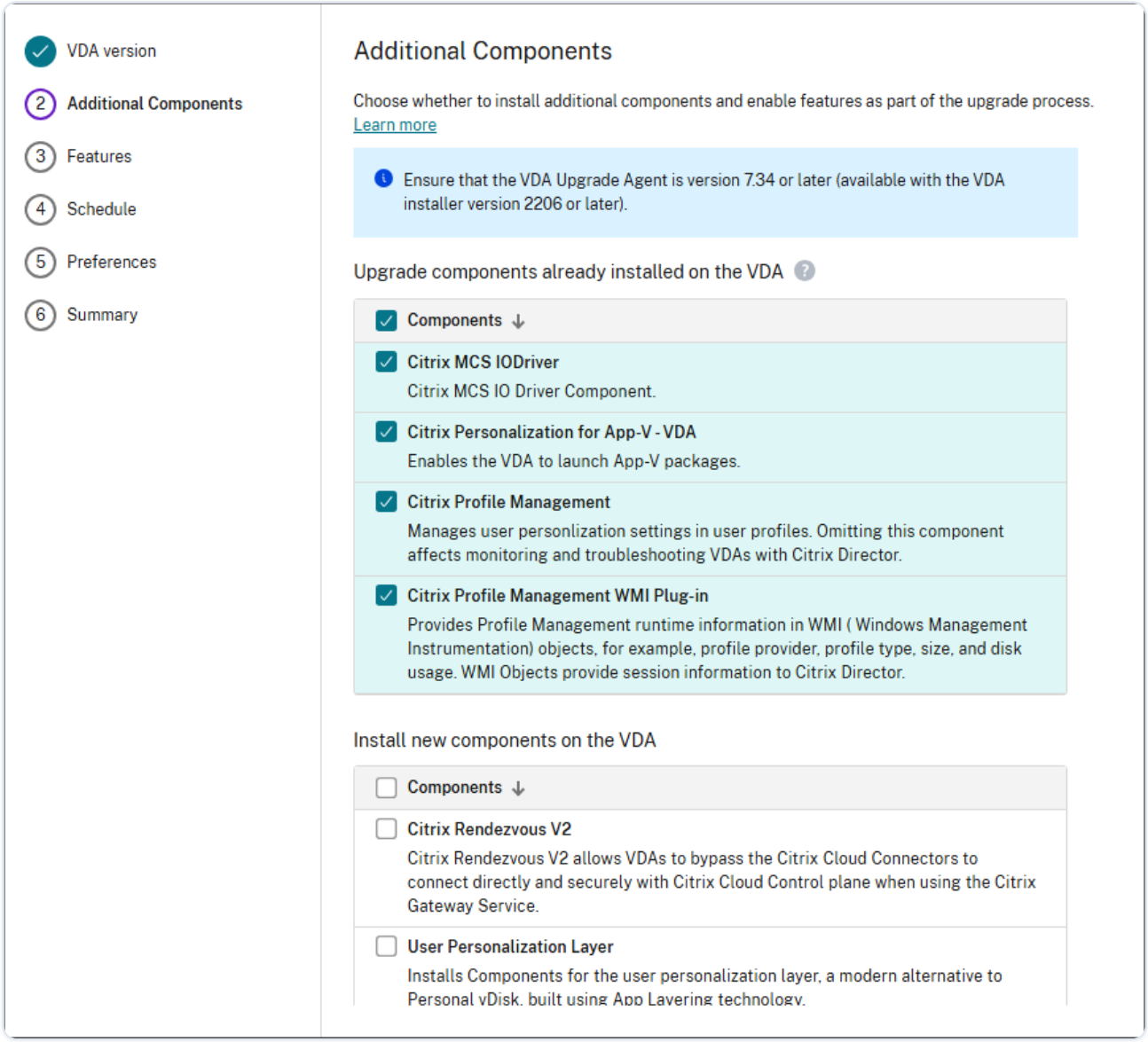
Por exemplo: `Get-VusAvailableVdaVersion -CatalogName '[Name of your Machine Catalog]'`

```
PS V:\> Get-VusAvailableVdaVersion -CatalogName 'CR-2303'

UpgradeType Version
----------- -------
         CR 2411.0.100.315
         CR 2407.0.100.274
         CR 2402.0.100.629
```

Componentes Adicionais

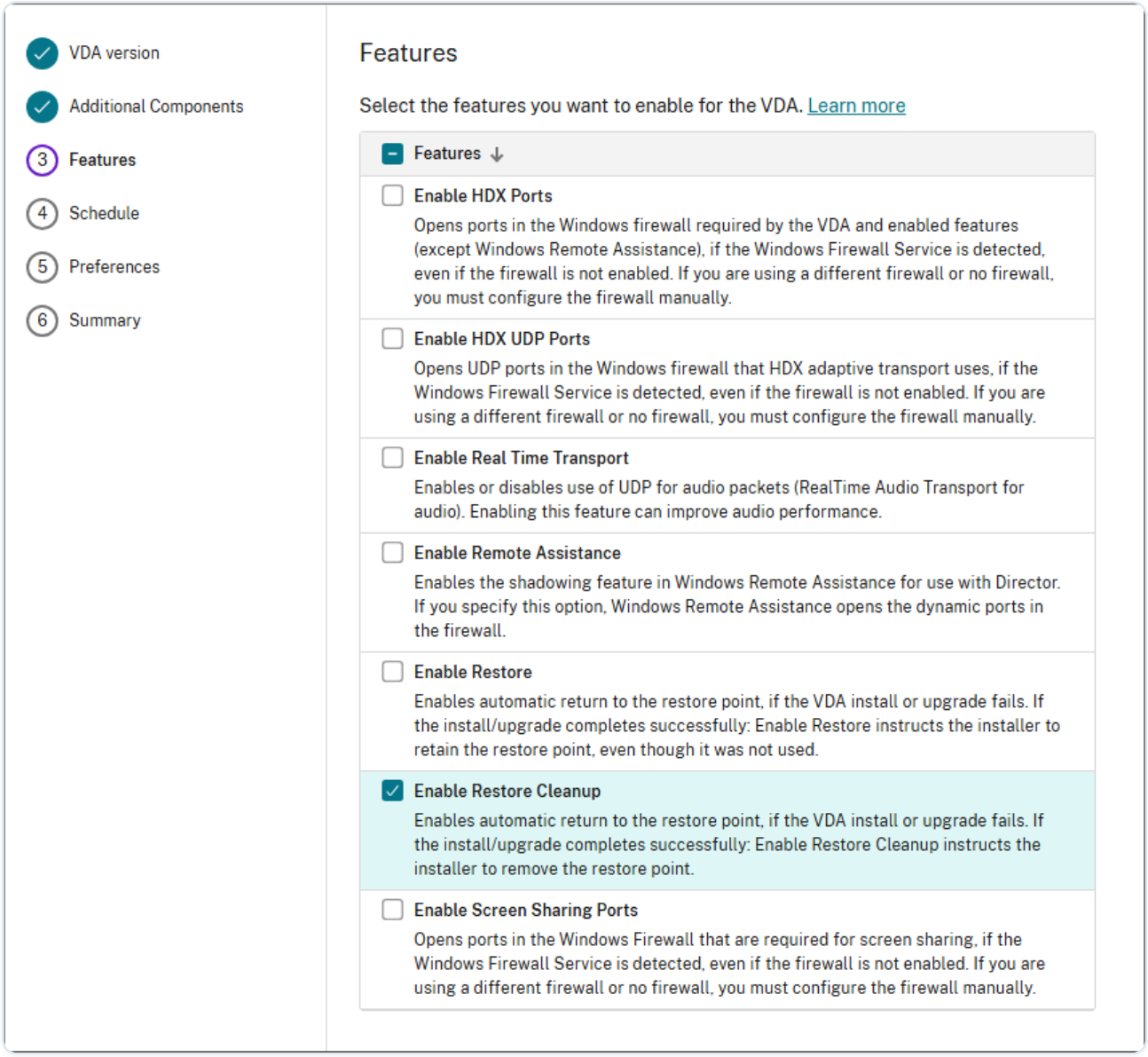
Componentes adicionais podem ser instalados ou atualizados ao atualizar VDAs por catálogo de máquinas ou por máquina individual. Se você não marcar um componente, ele não desinstalará o componente, mas o componente não será atualizado como parte da atualização geral do VDA.



Recursos

Os recursos podem ser habilitados ou atualizados em VDAs por meio do serviço de atualização de VDA. Se você não marcar um recurso, ele não desabilitará o recurso, mas o recurso não será atualizado como parte da atualização geral do VDA.

Por padrão, a caixa de seleção **Habilitar limpeza de restauração** está selecionada. A Citrix recomenda habilitar o recurso de limpeza de restauração para facilitar o gerenciamento e melhorar a recuperação de atualizações com falha. Com o recurso habilitado, um ponto de restauração do sistema é criado antes do início da atualização. Se uma atualização falhar, o VDA será restaurado para o ponto de restauração do sistema. O ponto de restauração é excluído após a instalação bem-sucedida do VDA. Para obter mais informações, consulte Restaurar em caso de falha de instalação ou atualização.



Nota:

A Restauração do Sistema do Windows é suportada apenas em sistemas operacionais de sessão única (por exemplo, Windows 10 e 11). O recurso Restauração do Sistema do Windows deve estar habilitado no VDA para que o recurso “Habilitar limpeza de restauração” funcione. As atualizações podem falhar se “Habilitar restauração” ou “Habilitar limpeza de restauração” for selecionado, mas a Restauração do Sistema do Windows não estiver configurada no VDA.

Simultaneidade

Ao atualizar catálogos de máquinas, o VUS permite definir um número máximo de VDAs que serão atualizados simultaneamente. Isso pode ajudar a reduzir a carga em sua conexão com a internet ou servidor de arquivos e, quando usado em conjunto com limites de falha, permite interromper as atualizações se um certo número de VDAs falhar na atualização.

Assim que a atualização agendada é iniciada, todos os VDAs no catálogo são colocados em modo de manutenção. Uma atualização será iniciada em uma quantidade de VDAs que corresponda à configuração máxima de simultaneidade definida. Assim que uma atualização de VDA for concluída, outro VDA começará a ser atualizado para manter o número simultâneo de VDAs sendo atualizados ao mesmo tempo.

Se nenhuma simultaneidade for especificada para uma atualização agendada de catálogo de máquinas, a Citrix usa um valor de simultaneidade padrão com base no número total de VDAs no Catálogo e na duração da atualização.

As atualizações levam em média cerca de 30 minutos para serem concluídas, mas isso pode variar muito com base nas condições ambientais. Considere definir sua simultaneidade para uma quantidade em que todos os VDAs possam ser atualizados na duração de atualização fornecida. Por exemplo, se você tiver 20 VDAs configurados para serem atualizados em 4 horas, você precisa de 5 VDAs para serem atualizados por hora. Usando a duração média de atualização de 30 minutos, você pode definir o valor de simultaneidade para 3 para atender ao requisito de 5 atualizações de VDA por hora (3 atualizações a cada 30 minutos resultam em 6 atualizações por hora).

Limite de Falha

Ao atualizar catálogos de máquinas, use um limite de falha para evitar que mais VDAs sejam atualizados se um determinado número de VDAs falhar. Os limites de falha podem reduzir o raio de impacto de problemas que causam falhas na atualização, diminuindo os esforços de solução de problemas para os administradores.

Os limites de falha impedem que quaisquer VDAs futuros iniciem atualizações, mas não interrompem os VDAs que já iniciaram a atualização. Por exemplo, se um catálogo de máquinas tiver 100 VDAs, a simultaneidade for definida como 10 VDAs e o limite de falha for definido como 3, se todas as atualizações de VDA falharem, pelo menos 13 VDAs terão tentado atualizar, e os 87 restantes nunca terão iniciado, e a atualização será cancelada.

10 VDAs simultâneos começam a ser atualizados no início da atualização agendada; se a primeira atualização falhar, outro VDA iniciará a atualização para manter as 10 atualizações simultâneas.

Se a segunda atualização falhar, outro VDA iniciará a atualização. Se a terceira atualização falhar, todos os VDAs que estão atualmente no processo de atualização continuarão, e o restante dos VDAs no agendamento de atualização terá sua atualização cancelada.

Local do Instalador do VDA

Você pode escolher que os VDAs baixem a mídia de instalação do VDA do CDN hospedado pela Citrix ou de um compartilhamento de arquivos local.

As atualizações por meio de um compartilhamento de arquivos hospedado localmente reduzem a necessidade de fornecer regras de rede para permitir que os VDAs busquem a mídia de instalação e podem diminuir a utilização da largura de banda durante o processo de atualização.

Se estiver usando o CDN hospedado pela Citrix, os VDAs devem ser capazes de se comunicar com as URLs listadas em Conectividade.

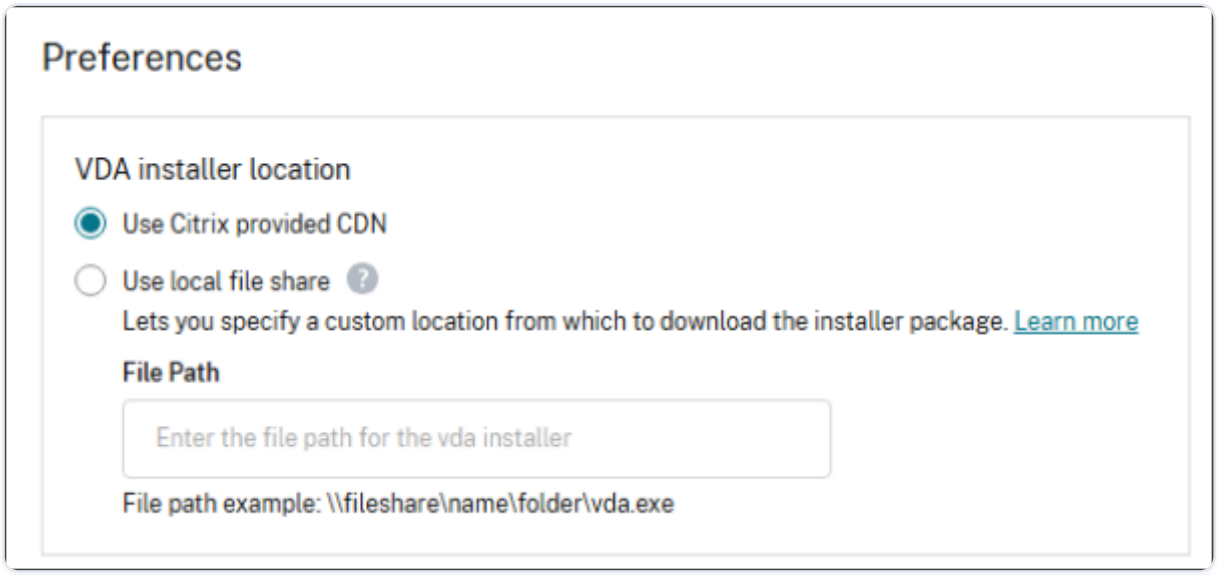
Se estiver usando um compartilhamento de arquivos local, o compartilhamento de arquivos deve ter os seguintes pré-requisitos.

- O Agente de Atualização VDA deve ser a versão 7.40.0.35 ou posterior, que é instalada por padrão na versão VDA 2311 ou posterior.
    - O Agente de Atualização VDA não requer uma atualização VDA agendada para ser atualizado. O Agente de Atualização VDA é atualizado automaticamente.
- Se a atualização for feita usando PowerShell, o SDK do PowerShell Remoto do Virtual Apps and Desktops versão 7.42 ou mais recente deve estar instalado.
- Permissões de Compartilhamento de Arquivos
    - Os compartilhamentos de rede que contêm pacotes de instalação VDA devem ter acesso de leitura para o serviço do Agente de Atualização VDA, que é executado como Sistema Local (principal NT AUTHORITY\SYSTEM).
    - VDAs Ingressados no Domínio:
        - A conta do Sistema Local (o VUA é executado como Sistema Local) usa credenciais de computador ao acessar compartilhamentos de rede.
        - O compartilhamento de arquivos deve ter acesso de leitura para Computadores do Domínio.
        - Em Configurações Avançadas de Compartilhamento, o **Compartilhamento de Arquivos e Impressoras** deve estar ativado.

    - VDAs Não Ingressados no Domínio:
        - A conta do Sistema Local (o VUA é executado como Sistema Local) usa **LOGON ANÔNIMO** ao acessar compartilhamentos de rede.
        - No **Centro de Rede e Compartilhamento, o Compartilhamento Protegido por Senha** deve estar desativado.
        - Na guia **Segurança** das permissões da pasta, as permissões de acesso de leitura devem ser concedidas ao **LOGON ANÔNIMO**.
        - Em Configurações Avançadas de Compartilhamento, o **Compartilhamento de Arquivos e Impressoras** deve estar ativado.
        - O nome da pasta compartilhada deve ser adicionado à **Política de Segurança de Acesso à Rede**.

- Instalador do VDA
    - O instalador do VDA deve ser baixado do site Citrix Downloads e colocado no compartilhamento de arquivos.
    - O instalador do VDA relevante para o catálogo de máquinas deve ser baixado.
        - Use o **instalador do VDA do SO multissessão** se o tipo de catálogo for multissessão.
        - Use o **instalador do VDA do SO de sessão única** se o tipo de catálogo for de sessão única.
    - Para uma determinada atualização, a versão do instalador no compartilhamento de arquivos deve corresponder exatamente a uma versão publicada pelo VUS. Use o cmdlet do PowerShell `Get-VusAvailableVersion` para determinar as versões disponíveis.

Para configurar VDAs para atualizar a partir de um compartilhamento de arquivos local na interface de Configuração Completa, selecione “Usar compartilhamento de arquivos local” no local do instalador do VDA e insira o caminho para o instalador. Por exemplo, `"\\hostname\VDA-Packages\VDAWorkstationSetup_2308.exe"`.



Para configurar VDAs para atualizar a partir de um compartilhamento de arquivos local usando o PowerShell, use o parâmetro `-VdaWorkstationPackageUri` (SO de sessão única) ou `-VdaServerPackageUri` (SO multissessão) ao agendar sua atualização.

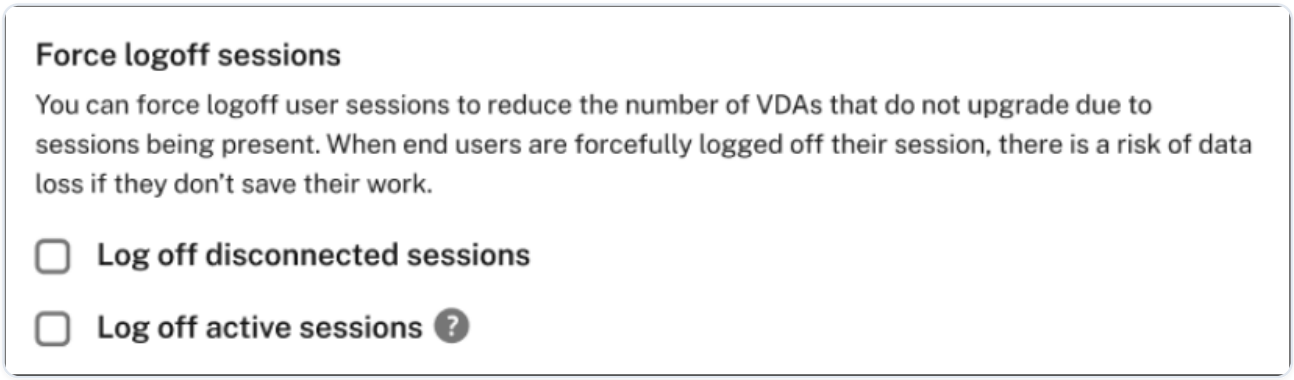
Forçar Logoff de Sessões

Para aumentar o número de VDAs disponíveis para atualização durante uma atualização agendada, considere forçar o logoff das sessões do usuário durante a atualização. O logoff forçado ocorre quando a atualização começa para cada VDA individual, e não no início da janela geral de atualização agendada.

Como diferentes VDAs começam a ser atualizados em momentos diferentes dentro do período agendado, os usuários só serão desconectados quando seu VDA específico iniciar a atualização.

Para forçar o logoff de sessões desconectadas durante atualizações agendadas usando a interface de Configuração Completa, selecione a opção **Fazer logoff de sessões desconectadas**.

Para forçar o logoff de sessões ativas durante atualizações agendadas usando a interface de Configuração Completa, selecione a opção **Fazer logoff de sessões ativas**. Se estiver fazendo logoff de sessões ativas, os usuários receberão uma notificação em sua sessão 10 minutos antes do início da atualização, lembrando-os de salvar seu trabalho antes de serem desconectados automaticamente.



Para forçar o logoff de sessões desconectadas durante atualizações agendadas usando PowerShell, use o parâmetro `-LogoffOption` ao agendar sua atualização. As opções disponíveis para `-LogoffOption` estão listadas abaixo:

- **ActiveSessionsOnly:** Se houver uma sessão ativa no VDA durante a janela de atualização agendada, o usuário será desconectado. Um banner será exibido 10 minutos antes do logoff do usuário para fornecer um aviso. VDAs com sessões desconectadas não serão desconectados durante a janela de atualização. Se a sessão desconectada permanecer durante toda a janela de atualização, essa atualização do VDA será cancelada.
- **DisconnectedSessionsOnly:** Se houver uma sessão desconectada no VDA durante a janela de atualização agendada, o usuário será desconectado. Os usuários não são notificados de que sua sessão desconectada será desconectada. VDAs com sessões ativas não serão desconectados durante a janela de atualização. Se a sessão ativa permanecer durante toda a janela de atualização, essa atualização do VDA será cancelada.
- **ActiveAndDisconnectedSessions:** Se houver uma sessão desconectada ou ativa no VDA durante a janela de atualização agendada, o usuário será desconectado. Para sessões ativas, um banner será exibido 10 minutos antes do logoff do usuário para fornecer um aviso.
- **DoNotLogoff:** Sessões ativas e desconectadas não são desconectadas. Se uma sessão estiver presente no VDA durante toda a duração do agendamento da atualização, a atualização será cancelada no final da janela de atualização agendada.

Quando possível, a Citrix recomenda forçar o logoff de sessões para aumentar o número de VDAs que são atualizados com sucesso.

> **Importante:**
>
> Forçar o logoff de sessões pode resultar na perda de trabalho não salvo pelos usuários em suas sessões.

Reiniciar VDAs antes de iniciar a atualização

Use a opção de reiniciar automaticamente os VDAs antes das atualizações para melhorar a taxa de sucesso, garantindo que cada VDA inicie o processo em um estado limpo e consistente. A reinicialização antes da atualização pode mitigar o risco de falhas comuns, como reinicializações pendentes, processos persistentes ou atualizações de sistema incompletas.

Quando esta opção está ativada, cada VDA é reiniciado individualmente pouco antes do início de sua atualização, em vez de no início da janela de atualização geral.

Para usar o recurso de reinicialização do VDA antes da atualização, o agente de atualização do VDA deve ser a versão 7.44 (lançada com o Citrix Virtual Apps and Desktops 2503) ou posterior. VDAs com uma versão anterior do Agente de Atualização do VDA serão atualizados sem uma reinicialização.

Ligar máquinas para atualizar VDA

Ao agendar uma atualização de VDA, você pode configurar o Serviço de Atualização de VDA para ligar automaticamente as máquinas que estão atualmente desligadas ou em hibernação no início da janela de atualização.

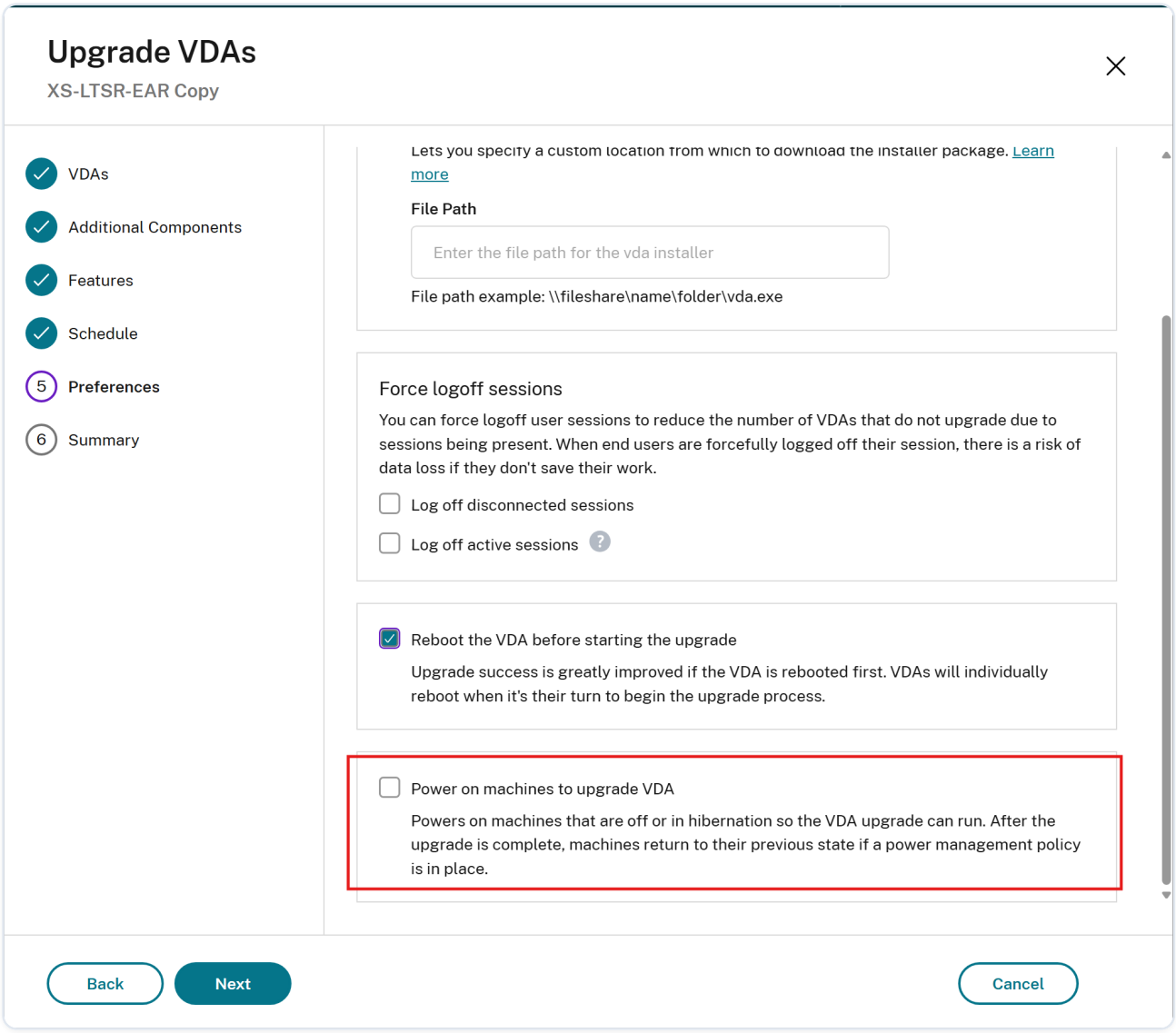
Por padrão, o Serviço de Atualização de VDA atualiza apenas máquinas que estão ligadas. Máquinas que estão desligadas ou hibernadas são ignoradas, o que pode deixar parte do seu catálogo executando uma versão mais antiga do VDA até a próxima janela de atualização. Ativar esta opção garante que essas máquinas sejam incluídas na execução da atualização.

Como funciona

No início da janela de atualização, o Serviço de Atualização do VDA liga todas as máquinas no escopo do agendamento que estão desligadas ou em hibernação, e então as atualiza junto com o restante do catálogo. Quando a atualização é concluída, cada máquina retorna ao seu estado de energia anterior — desde que uma política de gerenciamento de energia esteja configurada para o catálogo ou grupo de entrega. No entanto, o próprio serviço de atualização do VDA não desliga as máquinas.

Para habilitar esta opção

Ao criar ou editar um agendamento de atualização no Studio, selecione Ligar máquinas para atualizar o VDA nas opções de agendamento antes de confirmar o agendamento.



Nota:

As máquinas que já estão ligadas quando a janela de atualização começa não são afetadas por esta configuração.

As máquinas retornam ao seu estado de energia pré-atualização (desligadas ou hibernadas) somente se uma política de gerenciamento de energia estiver em vigor. Se nenhuma política for configurada, as máquinas permanecem ligadas após a conclusão da atualização.

Esta opção se aplica a agendamentos de atualização tanto em nível de catálogo quanto em nível de máquina.

Editar ou cancelar o fluxo de trabalho do VDA

Depois de agendar as atualizações para um catálogo, você pode editar a hora de início e a duração da atualização ou cancelá-la completamente.

Para editar ou cancelar uma atualização usando a interface do usuário no nível do catálogo de máquinas, clique com o botão direito do mouse em um catálogo de máquinas com uma atualização agendada existente e clique em **Editar Atualização Agendada do VDA**. Para editar uma atualização existente no nível do catálogo de máquinas usando o PowerShell, use os cmdlets `Set-VusCatalogUpgrade` e `Remove-VusCatalogUpgrade`.

Para editar ou cancelar uma atualização no nível da máquina, no nó de pesquisa, clique com o botão direito do mouse em uma máquina com uma atualização agendada existente e clique em **Editar Atualização Agendada do VDA**. Você não pode editar a atualização agendada do VDA para várias máquinas simultaneamente. Para editar uma atualização existente no nível da máquina usando o PowerShell, use os cmdlets `Set-VusMachineUpgrade` e `Remove-VusMachineUpgrade`.

Monitorar e Solucionar Problemas do VUS

Monitorando Atualizações Agendadas do VDA

VDAs e catálogos de máquinas possuem dois atributos para ajudar a monitorar a prontidão e o status atual das atualizações do VDA, que são visíveis como colunas que podem ser usadas para filtrar no Studio ou no painel de detalhes dos VDAs ou catálogos.

- Atualização do VDA
- Estado da Atualização do VDA

Atualização do VDA

A Atualização do VDA fornece informações sobre se o VDA ou o catálogo de máquinas tem o agente de atualização do VDA configurado e se os VDAs estão atualizados ou se uma atualização está disponível. Os status disponíveis são os seguintes:

ATUALIZAÇÃO DO VDA (STUDIO)	ATUALIZAÇÃO DO VDA (POWERSHELL)	DESCRIÇÃO
Nível do Catálogo		

ATUALIZAÇÃO DO VDA (STUDIO)	ATUALIZAÇÃO DO VDA (POWERSHELL)	DESCRIÇÃO
Não configurado	MissingUpgradeType	Uma trilha de atualização (CR, LTSR, CR EAR ou LTSR EAR) não foi selecionada para o catálogo de máquinas.
Agendado	AtualizaçãoAgendada	Uma atualização está agendada para o catálogo de máquinas.
Disponível	AtualizaçãoDisponível	Os VDAs no catálogo não estão na versão mais recente da trilha de atualização. Uma atualização é recomendada.
Atualizado	Atualizado	Os VDAs no catálogo estão na versão mais recente da trilha de atualização. Nenhuma ação é necessária, ou não há um destino de atualização disponível que suporte o sistema operacional atual do VDA.
Desconhecido	Desconhecido	Recuperando o estado mais recente da atualização do VDA.
Nível da Máquina		
Não configurado	TipoDeAtualizaçãoAusente	Uma trilha de atualização (CR, LTSR, CR EAR ou LTSR EAR) não foi selecionada para o catálogo de máquinas do VDA.
Agendado	UpgradeAgendado	Uma atualização está agendada para o VDA.

ATUALIZAÇÃO DO VDA (STUDIO)	ATUALIZAÇÃO DO VDA (POWERSHELL)	DESCRIÇÃO
Disponível	UpgradeDisponível	O VDA não está na versão mais recente da trilha de atualização. Uma atualização é recomendada.
Atualizado	Atualizado	O VDA está na versão mais recente da trilha de atualização. Nenhuma ação é necessária, ou não há um destino de atualização disponível que suporte o sistema operacional atual do VDA.
Verificando estado	Desconhecido	Recuperando o estado mais recente do Upgrade do VDA.

Nota:

- Para VDAs que usam a trilha LTSR, um catálogo só será exibido como Atualizado se os VDAs estiverem na atualização cumulativa (CU) mais recente da versão de serviço de longo prazo (LTSR) mais recente. Se o VDA estiver na CU mais recente de uma versão LTSR anterior, o Upgrade do VDA ainda será exibido como **Disponível**.
- Um VDA também é exibido como Atualizado quando nenhum destino de atualização disponível suporta seu sistema operacional atual (por exemplo, Windows Server 2016 do CVAD 2407 em diante). O assistente de Upgrade de VDAs então não oferece nenhum destino para o VDA. Para atualizá-lo, recrie a imagem da máquina para um sistema operacional suportado e, em seguida, agende a atualização. Consulte os Requisitos de sistema para a versão de destino e CTX224843.

Estado de Atualização do VDA

O Estado de Atualização do VDA fornece informações sobre o status de uma atualização agendada. Os status do Estado de Atualização do VDA são os seguintes:

ESTADO DE ATUALIZAÇÃO DO VDA (STUDIO)	ESTADO DE ATUALIZAÇÃO DO VDA (POWERSHELL)	DESCRIÇÃO
Nível do Catálogo		
Não agendado	NotScheduled	Nenhuma atualização está agendada para o catálogo.
Agendado	UpgradeScheduled	Uma atualização está agendada para o catálogo.
Em andamento	UpgradeInProgress	Uma atualização está em andamento para o catálogo.
Cancelado	UpgradeCancelled	Uma atualização foi cancelada para o catálogo. Isso pode ser devido a um cancelamento manual ou ao limite de falhas ter sido atingido.
Falhou	UpgradeFailed	Uma atualização agendada para o catálogo falhou.
Bem-sucedido	UpgradeSuccessful	Uma atualização agendada para o catálogo foi concluída com êxito. Observação: Uma atualização bem-sucedida não significa que todos os VDAs no catálogo foram atualizados com êxito.
-	Vazio	Nenhuma atualização agendada para o catálogo.
Nível da Máquina		
Agendado	UpgradeScheduled	Uma atualização está agendada para o VDA.
Aguardando atualização	UpgradeInUpgradeWindow	Uma atualização agendada está ativa, mas o VDA ainda não começou a ser atualizado. Consulte

ESTADO DE ATUALIZAÇÃO DO VDA (STUDIO)	ESTADO DE ATUALIZAÇÃO DO VDA (POWERSHELL)	DESCRIÇÃO
		“Simultaneidade” para obter mais informações sobre como as atualizações do VDA são balanceadas por carga.
Em andamento	UpgradeInProgress	O VDA está sendo atualizado no momento.
Cancelado	UpgradeCancelled	Uma atualização agendada foi cancelada para o VDA antes do início da atualização.
Atualização falhou	UpgradeFailed	O VDA começou a ser atualizado, mas a atualização não foi concluída com êxito. Consulte “solução de problemas” para obter mais informações.
Bem-sucedido	UpgradeSuccess	O VDA foi atualizado com sucesso.
A validação falhou	UpgradeValidationFailed	A validação do certificado falhou ao baixar os metadados para o instalador do VDA.
-	Vazio	Nenhuma atualização está agendada para o VDA.

Solução de problemas de atualizações agendadas do VDA

Se você encontrar falhas de atualização, os seguintes logs podem ajudá-lo a identificar e solucionar os problemas. Você também pode compartilhar esses logs com o Suporte Técnico da Citrix para agilizar o processo de assistência.

Logs de Instalação do VDA

Ao solucionar problemas de falhas de atualização, colete e revise os logs tanto para a instalação inicial do VDA quanto para a atualização com falha. Os logs de instalação e atualização podem ser encontrados nos seguintes locais.

- Os logs de instalação para instalações do VDA são colocados em:
  - %temp%/Citrix/XenDesktop Installer
- Os logs de atualização para instalações do VDA são colocados em:
  - C:\Windows\Temp\Citrix\XenDesktop Installer **ou**
  - C:\Windows\SystemTemp\Citrix\XenDesktop Installer

Versão do Agente de Atualização do VDA

Ao coletar dados para solucionar falhas de atualização através do VUS, é importante saber a versão do agente de atualização nos VDAs. Para verificar as versões do Agente de Atualização do VDA, use o seguinte cmdlet: `Get-VusComponentVersion -ComponentType VUS`. Ele lista todos os VDAs e suas versões do Agente de Atualização do VDA.

Para verificar as versões do Agente de Atualização do VDA no nível do catálogo, você pode usar o seguinte script:

> **Nota:**
>
> O script é fornecido como um exemplo e pode precisar ser adaptado para se adequar ao seu ambiente específico. Recomendamos que você teste o script completamente antes de usá-lo em um ambiente de produção.

```
Param( [Parameter (Mandatory=$true)] [string] $CatalogName ) try { $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-Object -Property UUID
```

```
if($Uuids -eq $null) { throw "Cannot find CatalogName " +$CatalogName } Write-Output("Catalog Name passed is "+$CatalogName)
```

```
foreach($Uuid in $Uuids) { $compVersion = Get-VusComponentVersion -MachineId $machine.UUID -ComponentType VUS $Machine = Get-BrokerMachine -UUID $compVersion.MachineId Write-Output(“MachineName: “+ $Machine.MachineName+”, Machine UUID:”+$machine.MachineId+”, VUA Version:”+ $compVersion.Version) } } catch { Write-Output(“Exception Occured”) Write-Host $_ }
```

Logs relacionados ao Agente de Atualização do VDA

Os logs do Agente de Atualização do VDA (VUA) podem fornecer informações essenciais para solucionar falhas de atualização e problemas com a comunicação do VUA com o serviço de atualização do VDA. Os logs que você pode coletar incluem:

- Rastreamentos do Citrix Diagnostic Facility (CDF). O nome do módulo CDF é VdaUpgradeAgent.
- Logs de eventos do Windows. Visualize os logs no Visualizador de Eventos > Logs do Windows > Aplicativos > Citrix VDA Upgrade Agent Service.

Para versões do VUA 7.44 e posteriores

Na versão 7.44 do Agente de Serviço de Atualização do VDA (incluída na versão 2503), uma configuração de registro está disponível que permite aos administradores habilitar um arquivo de log rotativo que captura informações críticas para solução de problemas, ao mesmo tempo que impede que os arquivos de log cresçam demais. O tamanho total dos arquivos de log é limitado a 20 MB. Crie a seguinte chave de registro para habilitar o registro em um arquivo:

- **Chave:**

  `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent -Name LogToFile -Value 1 -PropertyType DWord -Force`
- **Nome do valor:** `LogToFile`
- **Tipo de valor:** `REG_DWORD`
- **Dados do valor:**
  - `0` - rastreamento de arquivo desabilitado
  - `1` - rastreamento de arquivo habilitado

Para criar a chave de registro LogToFile em um VDA usando o PowerShell, use o seguinte cmdlet:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent -Name LogToFile -Value 1 -PropertyType DWord -Force
```

Para habilitar o LogToFile para grupos de máquinas em escala, considere criar o registro LogToFile em todas as unidades organizacionais (OUs) do VDA por meio da Preferência de Política de Grupo.

> **Observação:**
>
> - Quando `LogToFile=1` é definido, os logs são gravados apenas no arquivo. Eles não aparecerão nos rastreamentos CDF.
> - A reinicialização do serviço do Agente de Atualização do VDA é necessária para que a alteração do registro entre em vigor
> - O arquivo de log é criado na pasta C:\ProgramData\Citrix\Update Services\Logs

Para versões do VUA anteriores a 7.43

Se necessário, você pode modificar o arquivo de configuração do Agente de Atualização do VDA para que os logs sejam gravados continuamente em um arquivo. Para habilitar o registro em um arquivo, siga estas etapas:

1. Vá para a pasta `C:\Program Files\Citrix\CitrixUpgradeAgent`.
2. Abra o arquivo `Citrix.UpdateServices.UpdateAgent.exe.config`.
3. Altere o valor de `LogToFile` para `1`.
4. Reinicie o serviço Citrix VDA Upgrade Agent. Isso cria um arquivo de log em: `C:\ProgramData\Citrix\Update Services\Logs`.

> **Nota:**
>
> - Habilitar o registro em um arquivo através do arquivo .config grava logs continuamente, potencialmente consumindo espaço de armazenamento. Lembre-se de desabilitar o registro após a resolução do problema. Para desabilitar o registro, primeiro defina `LogToFile` como `0` e, em seguida, reinicie o Serviço Citrix VDA Upgrade Agent.

- Quando `LogToFile`=`1` é definido, os logs são gravados apenas no arquivo. Eles não aparecerão nos rastreamentos CDF.

Solucionar falhas de download da atualização do VDA

Siga as etapas abaixo para solucionar e resolver falhas de download relacionadas ao recurso de atualização do VDA:

1. Certifique-se de que as URLs relevantes foram adicionadas à lista de permissões se a filtragem de URL estiver em vigor. Consulte Requisito de atualização do VDA.
2. Após adicionar as URLs necessárias à lista de permissões, tente reagendar a atualização do VDA.

Você pode habilitar o rastreamento CDF ou definir `LogToFile` como `1` para capturar logs detalhados para análise. Se o problema de falha de download persistir, verifique os erros. Se você vir a seguinte mensagem de erro “Download Failed: This access control list is not in canonical form and therefore cannot be modified”, isso indica que as permissões na pasta `C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA` estão incorretas.

Para resolver o problema, faça uma das seguintes ações:

- **Opção 1:** Redefina as listas de controle de acesso (ACLs) na pasta usando o seguinte comando. (O comando redefine as ACLs com ACLs herdadas padrão para todos os arquivos correspondentes.)
  - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA" /reset /T /C /L /Q
- **Opção 2:** Exclua a pasta VDA em Downloads e, em seguida, agende a atualização do VDA.

Solucionar problemas de falhas de validação de atualização do VDA

Siga as etapas abaixo para solucionar e resolver falhas de download relacionadas ao recurso de atualização do VDA:

1. Certifique-se de que as URLs relevantes foram adicionadas à lista de permissões se a filtragem de URL estiver em vigor, especialmente as URLs da Lista de Revogação de Certificados (CRL) ou do Protocolo de Status de Certificado Online (OCSP) necessárias para a verificação de revogação. Consulte o requisito de atualização do VDA.
2. Depois de adicionar as URLs necessárias à lista de permissões, tente reagendar a atualização do VDA.

Sugerimos habilitar o rastreamento CDF ou definir LogToFile como 1 para capturar logs detalhados para análise. Os logs podem incluir os seguintes erros:

- RevocationStatusUnknown
- A função de revogação não conseguiu verificar o status de revogação do certificado.
- A função de revogação não conseguiu verificar a revogação porque o servidor de revogação estava offline.

O Agente de Atualização do VDA depende de chamadas de sistema do Windows para validar certificados e realizar verificações de revogação. Os erros acima indicam que o agente não consegue estabelecer uma conexão com as URLs CRL ou OCSP.

A CryptoAPI do Windows atualmente não oferece suporte a configurações de proxy. Revise a seção VDAs com configurações de proxy para configurar seus proxies VDA para facilitar chamadas CRL de saída.

Citrix DaaS™ para Citrix Service Providers

Este artigo descreve como os **Citrix Service Providers** (CSPs) podem configurar e gerenciar ambientes Citrix DaaS *multitenant* no Citrix Cloud. Ele também explica como os clientes locatários podem acessar e cogereciar seus ambientes atribuídos por meio de administração delegada.

Para uma visão geral dos recursos disponíveis para Parceiros Citrix, consulte Citrix Cloud for Partners.

O processo de configuração e gerenciamento envolve duas áreas principais:

- Gerenciar implantações DaaS multitenant como administradores parceiros: Como os CSPs (Parceiros) configuram e gerenciam ambientes DaaS multitenant no Citrix Cloud.
- Gerenciar seus recursos DaaS como administradores de locatário: Como os clientes locatários acessam e gerenciam seus próprios recursos DaaS em cooperação com os CSPs em implantações multitenant.

Requisitos

- Para configurar e gerenciar um ambiente Citrix DaaS multitenant no Citrix Cloud™, os **Parceiros** devem atender aos seguintes pré-requisitos:
  - Ter status de parceiro Citrix Service Provider
  - Ter uma conta Citrix Cloud™.
  - Ter uma assinatura Citrix DaaS multitenant ativa
- Para gerenciar os recursos DaaS de um locatário em um ambiente Citrix DaaS multitenant, os **administradores de locatário** devem atender aos seguintes pré-requisitos:
  - Ter uma conta Citrix Cloud criada por um CSP e adicionada ao serviço DaaS multitenant do CSP
  - Ser atribuído a uma função de administrador DaaS de locatário

Limitações

Esta seção descreve as limitações atuais no ambiente DaaS multilocatário do CSP.

- Os administradores de locatários podem criar e atualizar conexões de hospedagem somente depois que o administrador parceiro atribui uma zona ao escopo do locatário. Os administradores de locatários ainda não podem gerenciar tags porque os objetos de tag não são escopados.
- Se uma zona for atribuída ao escopo do locatário, o DaaS criará catálogos de máquinas nessa zona automaticamente. Se nenhuma zona for atribuída, o administrador parceiro deverá criar o primeiro catálogo de máquinas, atribuí-lo a uma zona e aplicar o escopo apropriado no console do Studio do parceiro.
- Os administradores de locatários não podem acessar os conjuntos de configuração do Workspace Environment Management™ (WEM). Um administrador parceiro deve atribuir o conjunto de configuração.
- As pastas em **Catálogos de máquinas** ainda não têm escopo definido, portanto, não são acessíveis aos administradores de locatários.

> **Nota:**
>
> O console do Studio do parceiro não impõe escopos automaticamente. Você é responsável por selecionar o escopo apropriado ao criar catálogos de máquinas, grupos de entrega e grupos de aplicativos para o locatário apropriado.

Administração de serviços para parceiros

Este artigo descreve como os Provedores de Serviços Citrix (Parceiros) configuram e gerenciam ambientes DaaS *multitenant* no Citrix Cloud.

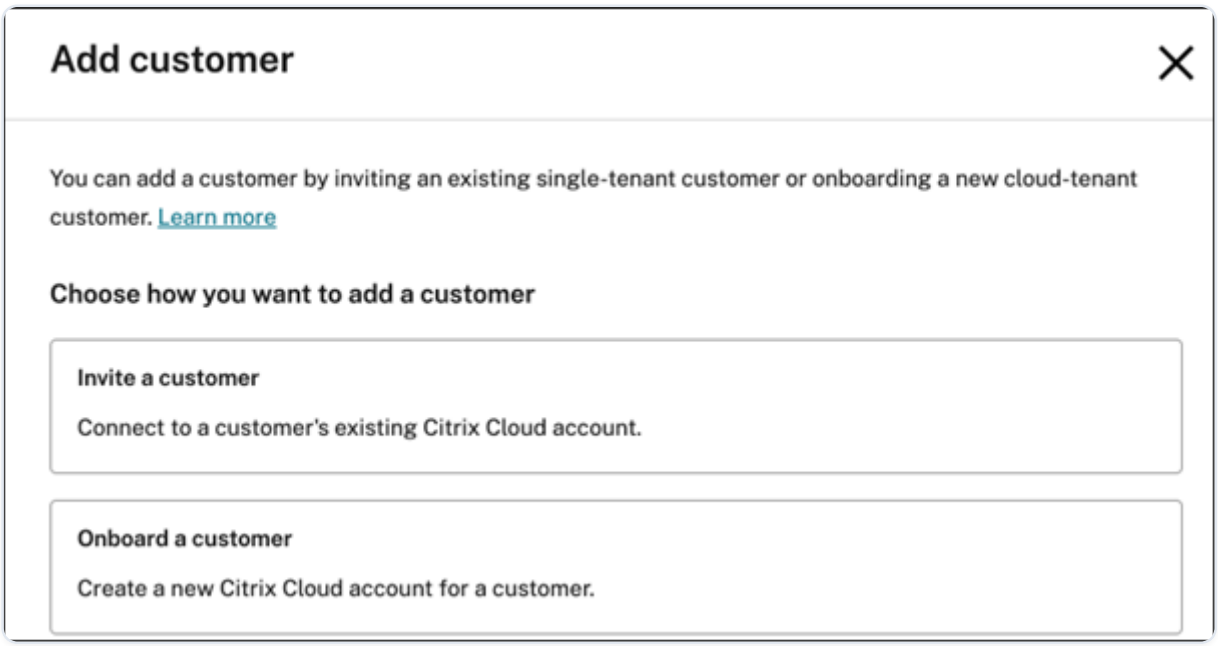
Para obter mais informações sobre os requisitos para parceiros CSP, consulte Requisitos.

> **Nota:**
>
> Para configurar uma implantação DaaS single-tenant e gerenciar os recursos DaaS deste cliente, siga o processo padrão descrito no guia de introdução do DaaS.

Etapa 1: Adicionar um cliente

Siga este procedimento para integrar um cliente *multitenant* que compartilha o ID da Org com o parceiro. As etapas também se aplicam para integrar um *single-tenant* que compartilha o ID da Org com o parceiro.

1. Faça login no Citrix Cloud com suas credenciais de Citrix Service Provider™ (CSP). Selecione **Meus Clientes** no menu superior esquerdo.
2. No painel **Meus Clientes**, selecione a guia **Cloud-tenant**, clique em **Adicionar cliente** e, em seguida, escolha **Integrar um cliente**.
3. Preencha os campos obrigatórios e clique em **Adicionar**.



Nota:

Adicionar o cliente cria uma conta de nuvem para o cliente e adiciona você (administrador parceiro) automaticamente como um administrador de acesso total desse inquilino.

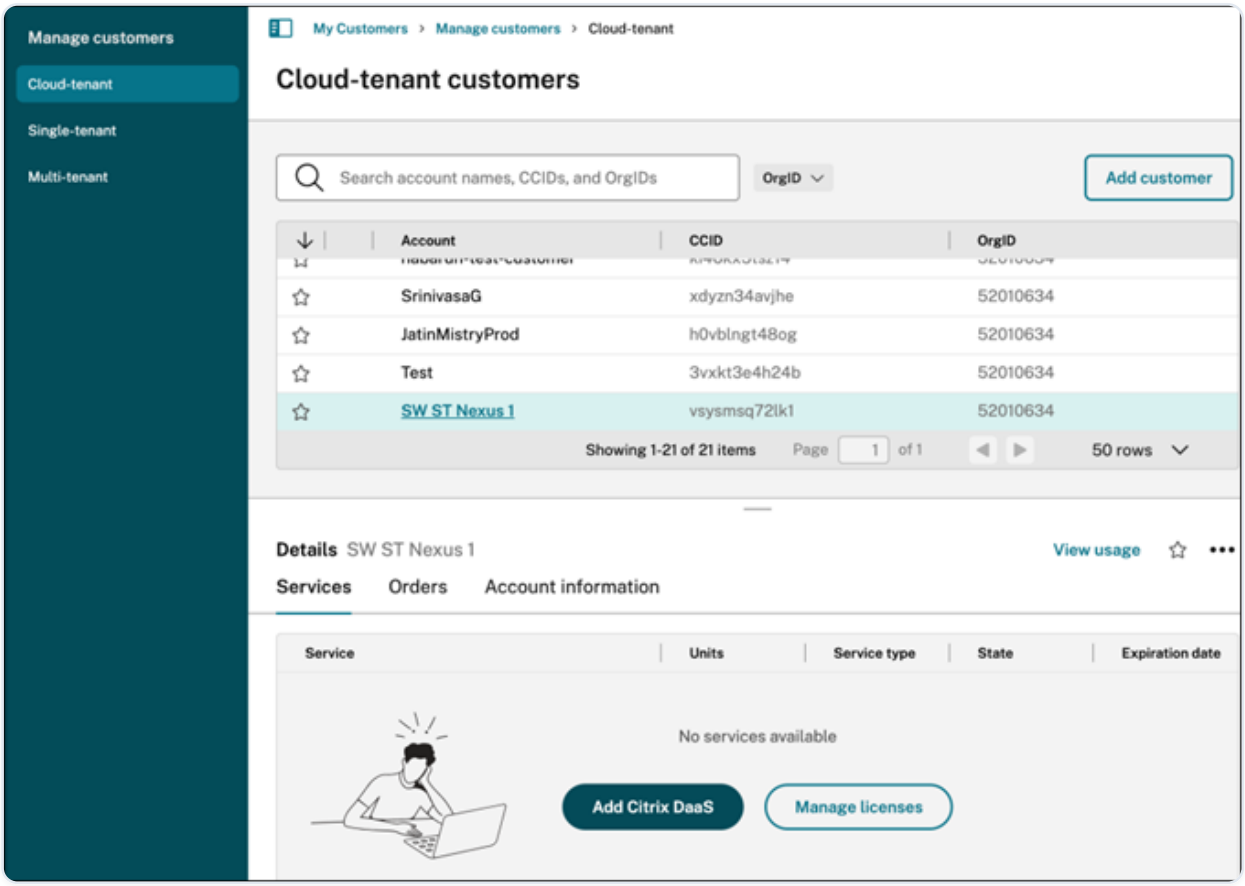
Para conectar um cliente *single-tenant* com um ID de Org autônomo e uma conta de nuvem existentes, siga estas etapas:

1. No painel **Meus Clientes**, selecione a guia **Cloud-tenant**, clique em **Adicionar cliente** e, em seguida, escolha **Convidar um cliente**.
2. Conecte-se com um cliente Citrix Cloud existente enviando a URL do Citrix Cloud para o cliente. Para mais informações, consulte Criar conexões com clientes. O cliente deve adicioná-

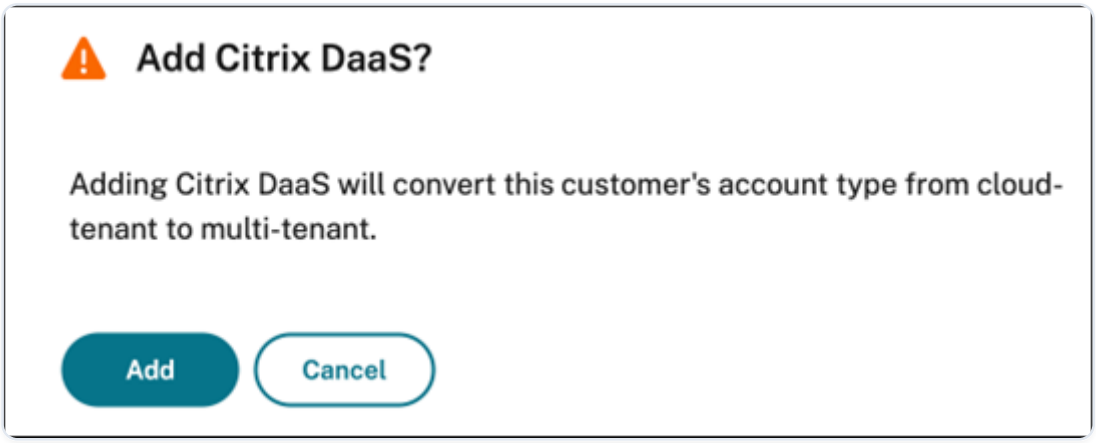
lo como administrador de acesso total à sua conta. Consulte Adicionar administradores a uma conta Citrix Cloud para mais informações.

Etapa 2: Adicionar o DaaS multilocatário Citrix® a um cliente

1. Faça login no Citrix Cloud com suas credenciais de CSP. Selecione **Meus Clientes** no menu superior esquerdo.
2. No painel **Meus Clientes**, vá para a guia **Locatário da Nuvem**, selecione o cliente e, no painel inferior **Detalhes** do cliente selecionado, clique em **Adicionar Citrix DaaS**.



3. Clique em **Adicionar** para confirmar.



> **Dica:**
>
> Se o administrador parceiro não conseguir executar **Adicionar DaaS** para um novo locatário, verifique se os seguintes requisitos são atendidos:
>
> - O administrador conectado tem permissões de acesso total na conta Citrix Cloud do locatário.
> - A conta do Citrix Service Provider tem o direito de DaaS multilocatário Citrix necessário.
>
> Após concluir este procedimento, o cliente é integrado à sua assinatura do Citrix DaaS.

Quando a integração é concluída, um novo escopo de cliente é criado automaticamente no Citrix DaaS. O escopo é visível na exibição do Studio. Este escopo é exclusivo para esse cliente. Você pode renomear o escopo, mas não pode excluí-lo.

Use este escopo para personalizar o acesso para outros administradores. Por exemplo, digamos que você tenha 10 clientes e dois administradores. Usando o escopo exclusivo, você pode restringir o acesso de um administrador a apenas três dos clientes. O outro administrador pode acessar um desses três clientes, mais dois outros clientes. Para detalhes, consulte Controlar o acesso do administrador aos clientes.

Etapa 3: Configurar um local de recurso

Um local de recurso contém as máquinas que entregam aplicativos e desktops para seus clientes, e componentes de infraestrutura como os Citrix Cloud Connectors. Para detalhes, consulte Conectar ao Citrix Cloud.

Em implantações DaaS multilocatário, os locatários são separados por locais de recurso e seus domínios associados. Embora cada locatário tenha sua própria conta de nuvem, todos os locais de recurso do locatário e seus conectores de nuvem devem ser implantados e gerenciados a partir da conta de parceiro do CSP. Para obter mais informações sobre arquitetura detalhada e opções de implantação, consulte Arquitetura de Referência DaaS do Provedor de Serviços Citrix.

Etapa 4: Federar domínios

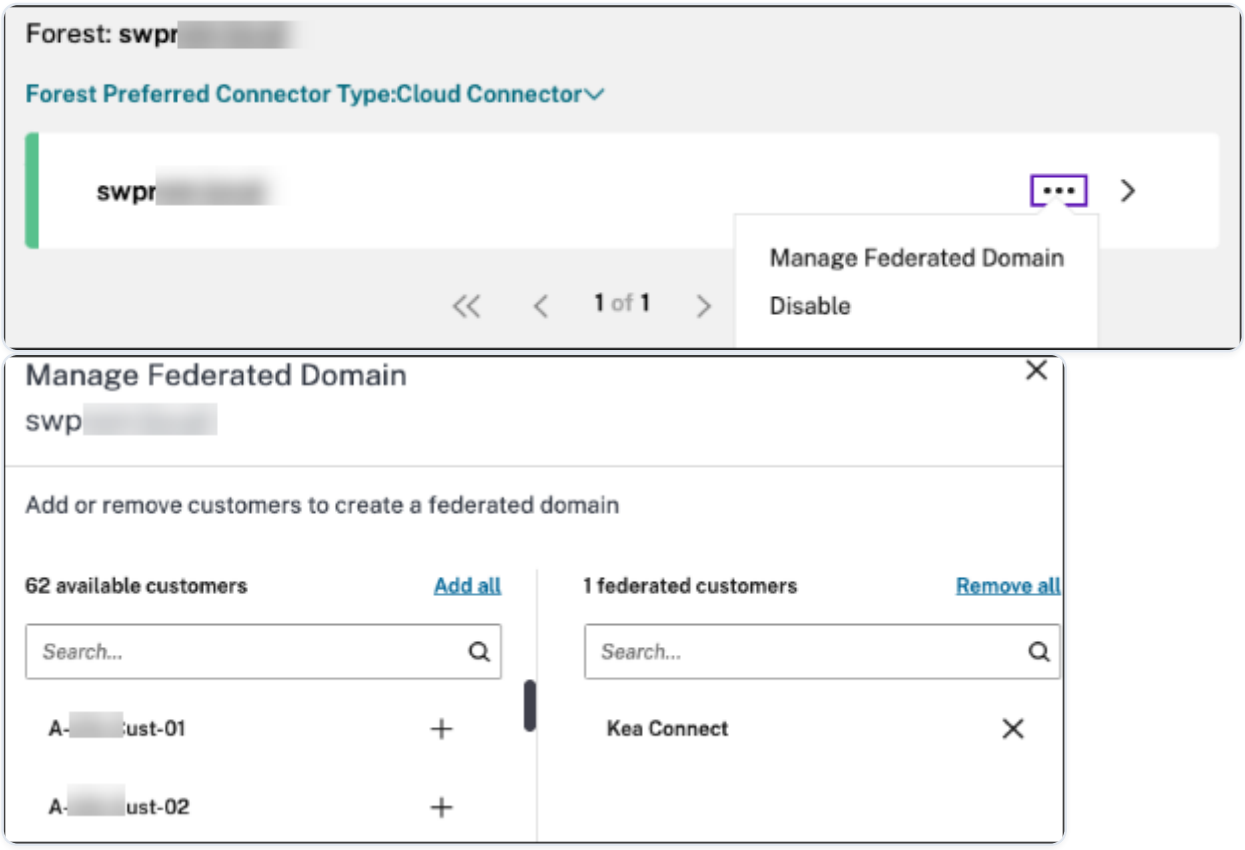
Domínios federados permitem que os usuários do cliente usem credenciais de um domínio anexado ao seu local de recurso designado ao cliente locatário para fazer login em sua loja. Esse comportamento permite que você forneça lojas dedicadas aos seus clientes que os usuários do

cliente podem acessar usando uma URL de loja personalizada definida na conta do locatário (*por exemplo*, customer.cloud.com), enquanto o local de recurso ainda está em sua conta Citrix Cloud. Você pode fornecer lojas dedicadas ao lado da loja compartilhada que os clientes podem acessar usando sua URL de loja CSP (*por exemplo*, csppartner.cloud.com).

Para permitir que os clientes acessem sua loja dedicada, adicione-os aos domínios apropriados que você gerencia. Depois de configurar a loja através do StoreFront Cloud, os usuários dos clientes podem fazer login em sua loja e acessar os aplicativos e desktops que você disponibilizou.

Adicionar um cliente a um domínio

1. Faça login no Citrix Cloud com suas credenciais CSP. Selecione **Identidade e Gerenciamento de Acesso** no menu superior esquerdo.
2. Na guia **Domínios**, localize o domínio relevante para o cliente e selecione **Gerenciar Domínio Federado** no menu de reticências do domínio.
3. No cartão **Gerenciar Domínio Federado**, na coluna **Clientes disponíveis**, selecione o cliente que você deseja adicionar ao domínio e clique no sinal de mais ao lado do nome do cliente. O cliente selecionado agora aparece na coluna **Clientes federados**. Repita para adicionar outros clientes. Quando terminar, selecione **Aplicar**.



Remover um cliente de um domínio

Ao remover um cliente de um domínio que você gerencia, os usuários do cliente não podem mais acessar suas lojas usando credenciais do seu domínio.

1. No menu do Citrix Cloud, selecione **Identidade e Gerenciamento de Acesso** e, em seguida, selecione **Domínios**.
2. Localize o domínio que você deseja gerenciar e selecione o botão de reticências. Selecione **Gerenciar Domínio Federado**.
3. Na lista de clientes federados, localize ou pesquise os clientes que deseja remover e selecione o botão X. Selecione **Remover todos** para remover todos os clientes da lista do domínio. Os clientes selecionados são movidos para a lista de clientes disponíveis.
4. Selecione **Aplicar**.
5. Revise os clientes que você selecionou e selecione **Remover Clientes**.

Etapa 5: Atribuir uma zona ao escopo do locatário

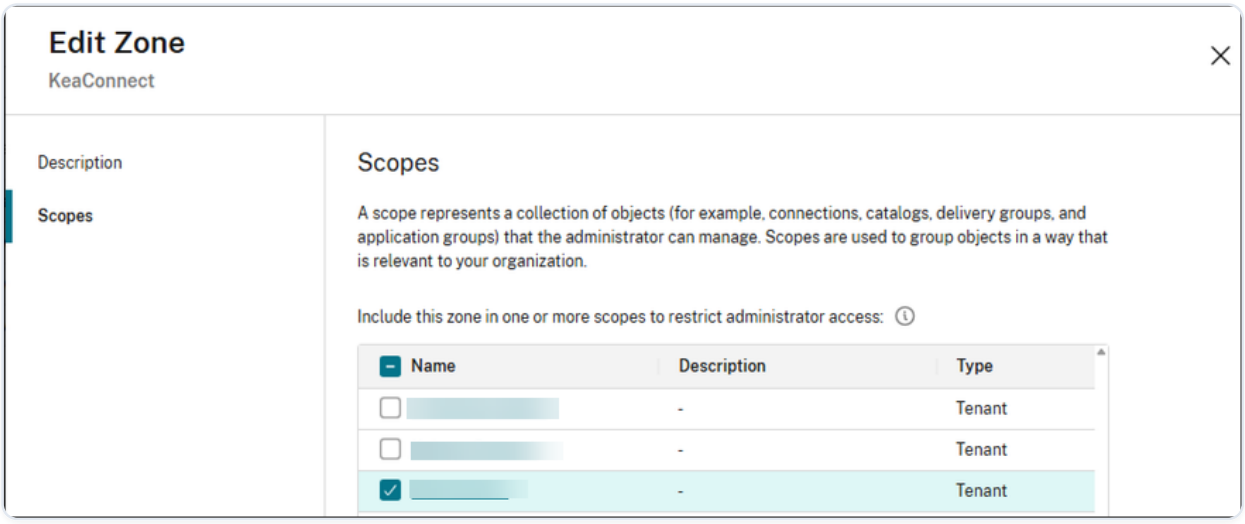
As zonas agora podem ser definidas para um locatário. Depois de atribuir uma zona ao escopo de um locatário, o administrador do locatário pode gerenciar suas próprias conexões de hospedagem e catálogos de máquinas dentro dessa zona. Atribua a zona que corresponde ao local de recurso que você configurou para o locatário.

Para atribuir uma zona ao escopo de um locatário:

1. No console do Citrix DaaS Studio, vá para **Gerenciar > Zonas**.
2. Selecione a zona cujo nome corresponde ao local de recurso do locatário e, em seguida, selecione **Editar zona**.



3. Na guia **Escopos**, selecione o escopo do locatário e, em seguida, selecione **Salvar**.



Etapa 6: Criar um conjunto de políticas para o escopo do locatário

Os administradores de locatários podem gerenciar políticas apenas dentro de um conjunto de políticas que você atribui ao escopo deles. Para permitir que um locatário gerencie políticas de forma independente, crie um conjunto de políticas e atribua-o ao escopo do locatário. O administrador do locatário pode então criar e gerenciar políticas dentro desse conjunto de políticas.

Os conjuntos de políticas não são habilitados por padrão. Para usar esse recurso, primeiro habilite os conjuntos de políticas, e depois crie um conjunto de políticas e atribua-o ao escopo do locatário.

Etapa 7: Configurar catálogos e grupos para entregar aplicativos e desktops

> **Nota:**
>
> Para gerenciar o DaaS para um cliente locatário como administrador parceiro, você deve mudar para a conta de nuvem do CSP. Para fazer isso, clique no nome da conta no menu superior direito e clique em **Mudar cliente**.

> Um catálogo é um grupo de máquinas virtuais idênticas. Ao criar um catálogo, uma imagem é usada (com outras configurações) como um modelo para criar as máquinas. Para obter detalhes, consulte Criar catálogos de máquinas.

Um grupo de entrega é uma coleção de máquinas selecionadas de um ou mais catálogos de máquinas. O grupo de entrega especifica quais usuários podem usar essas máquinas, além dos

aplicativos ou desktops disponíveis para esses usuários. Para obter detalhes, consulte Criar grupos de entrega.

Os grupos de aplicativos permitem que você gerencie coleções de aplicativos. Você pode criar grupos de aplicativos para aplicativos compartilhados entre diferentes grupos de entrega ou usados por um subconjunto de usuários dentro de grupos de entrega. Para obter detalhes, consulte Criar grupos de aplicativos.

Os catálogos de máquinas e os grupos de entrega para locatários podem ser criados de duas maneiras: o administrador parceiro os cria na conta do parceiro e os atribui aos escopos de locatário relevantes, ou os administradores de locatários os criam a partir de suas próprias contas de nuvem de locatário.

Ao configurar grupos, certifique-se de que:

- O escopo do grupo de entrega é um subconjunto do escopo do catálogo de máquinas. Por exemplo, suponha que o escopo do catálogo seja A e B. O escopo do grupo de entrega pode ser A ou B, ou A e B.
- O escopo do grupo de aplicativos é um subconjunto do escopo do grupo de entrega. Por exemplo, suponha que os grupos de entrega associados a um grupo de aplicativos tenham escopo A e B. O escopo do grupo de aplicativos pode ser A ou B, ou A e B.
- Para considerações de segurança em uma implantação multilocatário, é recomendável separar todos os objetos precedentes por escopos de locatário específicos.

> **Nota:**
>
> O console do Studio do parceiro não impõe escopos automaticamente. Você é responsável por selecionar o escopo apropriado ao criar catálogos de máquinas, grupos de entrega e grupos de aplicativos para o locatário apropriado.

Etapa 8: Controlar o acesso do administrador aos clientes

Você pode controlar o acesso do administrador aos clientes usando o escopo exclusivo que foi criado quando você adicionou o Citrix DaaS ao cliente. Você pode configurar o acesso ao adicionar um administrador ou posteriormente.

Para saber mais sobre como restringir o acesso usando funções e escopos no Citrix DaaS, consulte Administração delegada.

Adicionar um administrador parceiro com acesso restrito

1. Faça login no Citrix Cloud com suas credenciais CSP e selecione sua conta de parceiro na lista de contas disponíveis.
2. Selecione **Gerenciamento de Identidade e Acesso** no menu superior esquerdo.
3. Na guia **Administradores**, selecione **Adicionar Administradores De** e, em seguida, selecione **Citrix Identity**.
4. Digite o endereço de e-mail da pessoa que você está adicionando como administrador e, em seguida, selecione **Convidar**.
5. Configure as permissões de acesso apropriadas para o administrador. A Citrix recomenda selecionar **Acesso personalizado**, a menos que você queira que o administrador tenha controle de gerenciamento do Citrix Cloud e de todos os serviços assinados.
6. Depois de selecionar **Acesso personalizado**, selecione um ou mais pares de função e escopo para o Citrix DaaS, conforme necessário. Certifique-se de habilitar apenas as entradas que contêm o escopo exclusivo que foi criado para o cliente.
7. Quando terminar de selecionar os pares de função e escopo, selecione **Enviar Convite**.

Quando o administrador aceitar o convite, ele terá o acesso que você atribuiu.

Editar permissões de administração delegada para administradores

1. Faça login no Citrix Cloud com suas credenciais CSP e selecione sua conta de parceiro na lista de contas disponíveis.
2. Selecione **Gerenciamento de Identidade e Acesso** no menu superior esquerdo.
3. Na guia **Administradores**, selecione **Editar Acesso** no menu de reticências para o administrador.
4. Selecione e desmarque os pares de função e escopo para o Citrix DaaS, conforme necessário. Certifique-se de habilitar apenas as entradas que contêm o escopo exclusivo que foi criado para o cliente.
5. Selecione **Salvar**.

Visualizar administradores DaaS e suas funções e escopos atribuídos

1. Faça login na sua conta de parceiro do Citrix Cloud com suas credenciais CSP.
2. Selecione o bloco **DaaS** no menu superior esquerdo.
3. Selecione **Administradores** no painel esquerdo.

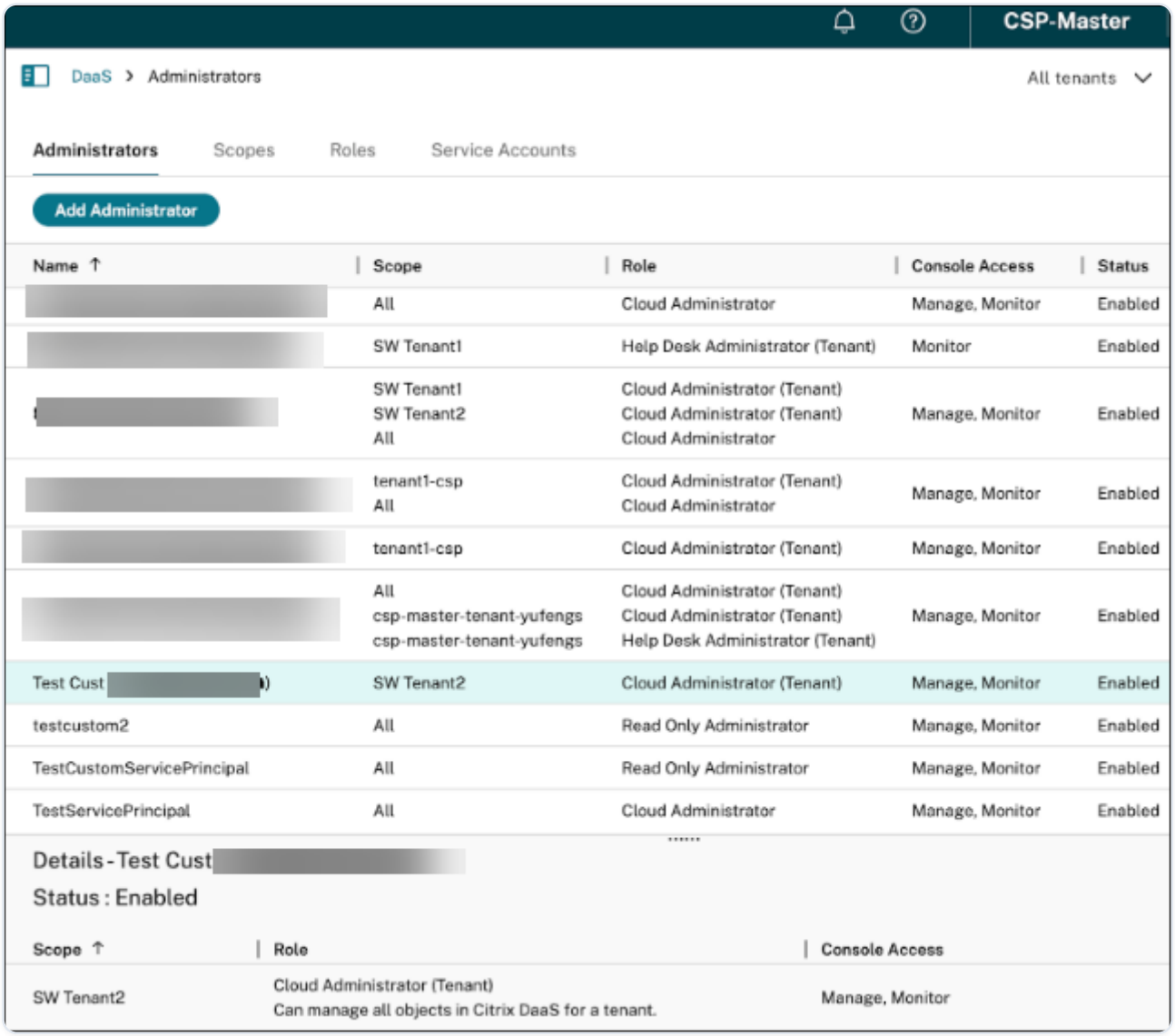
As informações estão disponíveis em três guias:

- A guia **Administradores** lista os administradores que foram criados, além de suas funções e escopos.
- A guia **Funções** lista todas as funções. Para visualizar os detalhes da função, selecione a função no painel do meio. A parte inferior desse painel lista os tipos de objeto e as permissões associadas à função. Selecione a guia **Administradores** no painel inferior para exibir uma lista de administradores que atualmente possuem esta função.
- A guia **Escopos** lista todos os escopos, incluindo os escopos gerados para clientes de parceiros Citrix.

Exportar atividades do administrador para auditoria

Em um ambiente Citrix DaaS multilocatário, vários clientes locatários compartilham uma instância DaaS. Cada locatário tem seu próprio acesso administrativo com escopo. Obter visibilidade sobre funções e escopos ajuda a garantir a delegação segura e simplifica a auditoria.

Todas as funções de administrador de nível de locatário definidas nas contas de locatário são sincronizadas automaticamente com o painel **Administradores** no console do Studio do parceiro. Um administrador parceiro com **Acesso total** pode exportar os dados como um arquivo CSV para relatórios e análises.



Para mais auditoria, o histórico de atividades do administrador também pode ser exportado do nó **Registro** no Studio.

Etapa 9: Configurar lojas

Um cliente pode ter sua própria loja com um `customer.cloud.com` exclusivo ou URL personalizado definido na conta de nuvem do cliente. Esta loja é onde os usuários do cliente acessam seus aplicativos e desktops publicados. Alternativamente, o CSP pode compartilhar sua URL de loja com a marca do parceiro com vários clientes locatários.

Para visualizar ou configurar URLs de loja compartilhada do parceiro:

1. Faça login na sua conta de parceiro do Citrix Cloud com suas credenciais CSP.
2. Selecione **StoreFront Cloud** no menu superior esquerdo.

Você pode alterar o acesso e a autenticação a uma loja. Você também pode personalizar a aparência e as preferências da loja. Para obter detalhes, consulte os seguintes artigos:

- Personalize sua experiência de loja
- Autenticação

Para visualizar ou configurar a URL da loja de um cliente locatário:

1. Faça login na conta do Citrix Cloud do cliente locatário.
2. Vá para **StoreFront Cloud**.

Nota:

- Para qualquer método de autenticação usado na conta do locatário, o administrador parceiro deve primeiro habilitar o mesmo método na conta CSP pai em **Gerenciamento de Identidade e Acesso** antes que ele possa ser configurado na conta do locatário.
- Em cenários onde o Citrix Federated Authentication Service (FAS) é implantado para processar SSO para usuários em um ambiente multilocatário, consulte a documentação de suporte multilocatário do FAS para obter mais informações.

Monitorar o serviço de um cliente

Em um ambiente CSP, o painel **Monitor** funciona da mesma forma que em um ambiente não CSP, mas exibe vários escopos de locatário na mesma instância DaaS. Para obter mais informações, consulte Monitor para detalhes.

Por padrão, o painel **Monitor** exibe dados para todos os clientes locatários. Para visualizar informações de um locatário específico, selecione o escopo do locatário na lista suspensa **Todos os locatários** no canto superior direito.

Tenha em mente que a capacidade de um administrador parceiro de ver as exibições do Monitor para um cliente é controlada pelo acesso configurado do administrador completo. O acesso deve incluir um par de função e escopo que inclua o escopo exclusivo do cliente.

Se você usou funções integradas para configurar o acesso: As funções integradas controlam se o administrador pode ver as exibições do Studio. Se você selecionar apenas pares de função e escopo de cliente que não incluem visibilidade do nó **Monitor**, esse administrador não poderá ver o nó **Monitor** para nenhum cliente selecionado. Por exemplo, se você conceder a um administrador acesso de **Administrador Somente Leitura,customerABC**, esses administradores parceiros não poderão ver o nó **Monitor** para **customerABC**, porque administradores somente leitura não podem acessar as exibições do Monitor.

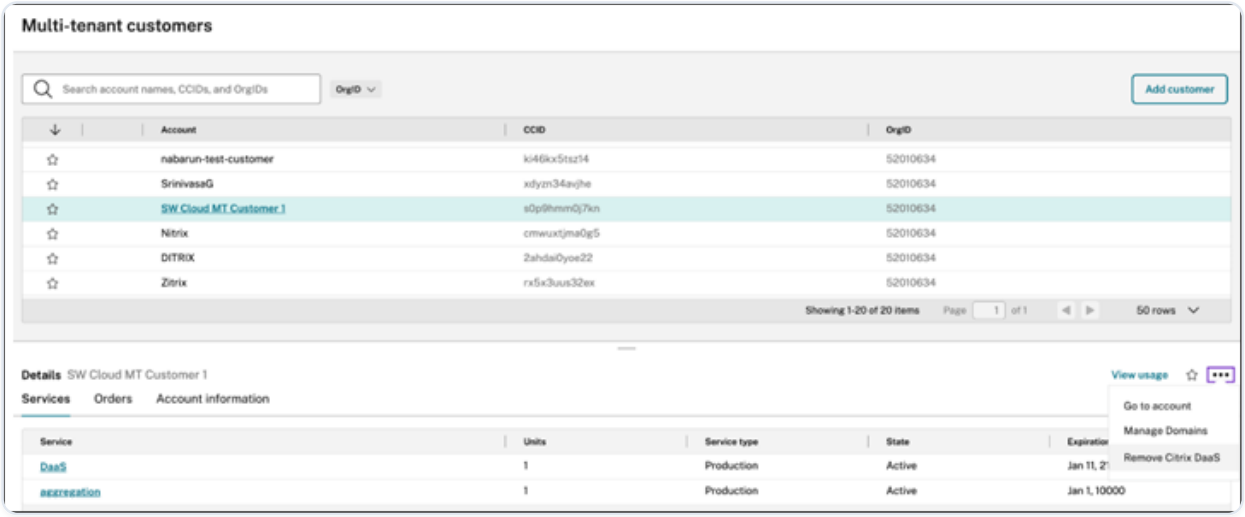
Remover o serviço DaaS de um cliente

Pré-requisitos:

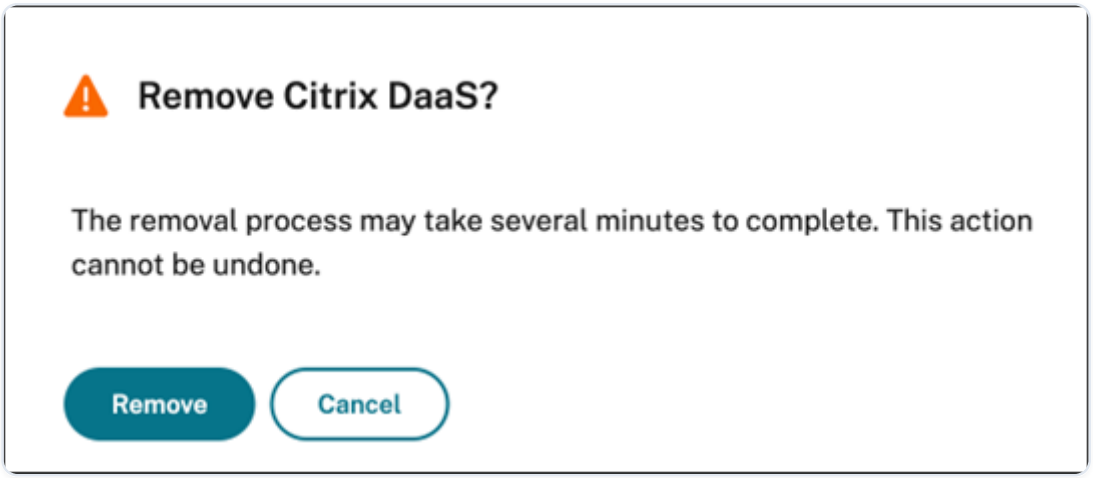
- Certifique-se de que o escopo do seu cliente não esteja vinculado a nenhum objeto do Citrix DaaS. Se estiverem vinculados, você não poderá remover o serviço. Para desvincular escopos, vá para **Studio > Administradores > Escopos** e edite o escopo.
- Para saber o escopo do seu cliente e gerenciá-lo, consulte Criar e gerenciar escopo.

Para remover o serviço DaaS de um cliente:

1. Faça login na sua conta de parceiro do Citrix Cloud com credenciais de administrador parceiro com permissões de **Acesso total** no cliente.
2. No painel **Meus Clientes**, vá para a guia **Multi-tenant**, localize o cliente, clique no menu de reticências (…) ao lado do cliente e selecione **Remover Citrix DaaS**.



A seguinte caixa de diálogo é exibida.



3. Clique em **Remover** para remover o serviço.



Administração do serviço de locatário

Este artigo descreve como os clientes locatários acessam e gerenciam seus próprios recursos DaaS em cooperação com os Provedores de Serviços Citrix (CSPs) em uma implantação *multilocatário*.

Adicionar administradores de locatário

Em um ambiente multilocatário, os administradores de clientes locatários devem ser adicionados apenas na conta Citrix Cloud de cada locatário. Adicionar administradores de locatário à conta de parceiro do Provedor de Serviços Citrix (CSP) *não* é suportado porque não garante o isolamento de segurança adequado.

O primeiro administrador de locatário deve ser adicionado por um administrador parceiro que criou inicialmente a conta do locatário. Depois disso, este administrador de locatário com acesso total pode adicionar mais administradores de locatário.

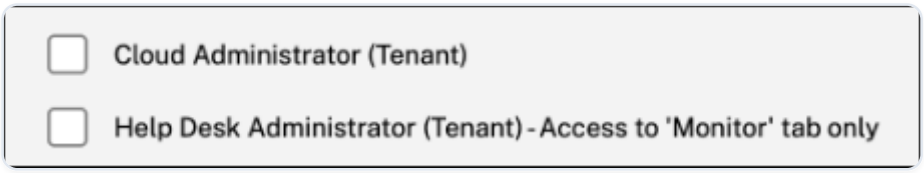
Para adicionar um administrador de locatário:

1. Faça login na conta Citrix Cloud™ do cliente locatário como um administrador de locatário com permissão de **Acesso total** no locatário.
2. Siga as etapas em Convidar administradores individuais.
3. Atribua uma das seguintes permissões ao administrador de locatário conforme necessário:

    - **Administrador da Nuvem (Locatário)**: Tem permissões totais para gerenciar os próprios catálogos de máquinas, grupos de entrega e outros objetos com escopo do locatário. Para atribuir esta função, faça um dos seguintes:

        - Selecione **Acesso total**.
        - Selecione **Acesso personalizado**, depois selecione **Administrador da Nuvem (Locatário)** em DaaS.

    - **Administrador de Help Desk (Locatário):** Tem acesso apenas ao console Monitor. Para atribuir esta função, selecione **Acesso personalizado**, depois selecione **Administrador de Help Desk (Locatário)** em DaaS.



Nota:

- Administradores adicionados na conta do locatário são automaticamente sincronizados com o console do Studio do parceiro com a função e o escopo apropriados.
- Não é recomendado que os administradores parceiros façam login na conta de nuvem de um cliente locatário para gerenciamento de DaaS. Certos recursos são bloqueados em contas de locatário por motivos de segurança.
- Para entender as diferenças de permissão entre **Administrador de Nuvem (Locatário)** e **Administrador de Help Desk (Locatário)**, consulte a tabela a seguir **Recursos disponíveis por função de administrador de locatário**.

Acessar o console do Studio na conta do locatário

Como administrador de locatário, você pode acessar uma experiência do Studio com escopo diretamente da conta do Citrix Cloud do cliente locatário.

1. Faça login na conta do Citrix Cloud do cliente locatário.
2. Selecione **DaaS** na página inicial ou no menu superior esquerdo. O console do Studio é aberto com a funcionalidade baseada na função atribuída ao administrador.

   Estúdio do locatário(/en-us/citrix-daas/media/tenant-studio.png)

O console exibe apenas objetos e configurações dentro do escopo do locatário. Objetos sem escopo não são acessíveis a partir da visualização do locatário.

Tabela: Recursos disponíveis por função de administrador de locatário

FUNÇÃO	ADMINISTRADOR DE NUVEM (LOCATÁRIO)	ADMINISTRADOR DE HELP DESK (LOCATÁRIO)
Início	Sim	Não aplicável
Pesquisar	Sim	Sim

FUNÇÃO	ADMINISTRADOR DE NUVEM (LOCATÁRIO)	ADMINISTRADOR DE HELP DESK (LOCATÁRIO)
Catálogos de Máquinas	Sim	Não aplicável
Grupos de Entrega	Sim	Não aplicável
Aplicativos	Sim	Não aplicável
Políticas	Gerenciar apenas conjuntos de políticas personalizados	Não aplicável
Administradores	Sim	Não aplicável
Hospedagem	Sim	Não aplicável
Monitor	Sim	Sim
Gravação de Sessão	Sim	Não aplicável
Downloads	Sim	Não aplicável
Configurações	Apenas minhas preferências	Não aplicável

Atualizar conexões de host

Depois que o administrador parceiro atribui uma zona ao escopo do seu locatário, você pode criar ou atualizar conexões de hospedagem dentro dessa zona como um administrador de locatário com a função de **Administrador de Nuvem (Locatário)**.

Criar catálogos e grupos de entrega

Como um administrador de locatário com a função de **Administrador de Nuvem (Locatário)**, você pode gerenciar catálogos de máquinas e grupos de entrega dentro do seu escopo atribuído.

Se o administrador parceiro atribuir uma zona ao seu escopo, o DaaS cria automaticamente todos os seus catálogos de máquinas nessa zona. Se nenhuma zona for atribuída ao seu escopo, o administrador parceiro deve criar o *primeiro* catálogo de máquinas para o seu escopo para garantir que a zona inicial correta seja selecionada para o seu catálogo.

Gerenciar políticas na conta do locatário

Por padrão, conjuntos de políticas integrados são visíveis em todos os escopos no console do Studio do parceiro.

Se um locatário precisar gerenciar políticas de forma independente:

1. Na **conta do parceiro**, um administrador parceiro deve criar um **conjunto de políticas personalizado** com escopo para esse locatário.
2. Na **conta do locatário**, administradores de locatário com a função de **Administrador de Nuvem (locatário)** gerenciam políticas dentro desse conjunto.

Citrix Gateway

O Citrix Gateway fornece aos usuários acesso seguro a aplicativos Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™).

O serviço Citrix Gateway permite acesso seguro e remoto a esses aplicativos, sem a necessidade de implantar o Citrix Gateway na DMZ ou reconfigurar seu firewall. A sobrecarga de infraestrutura do uso do Citrix Gateway é transferida para o Citrix Cloud.

Para obter mais informações sobre o serviço Citrix Gateway, consulte a documentação do produto. Esse conteúdo inclui como habilitar o serviço Citrix Gateway e problemas conhecidos para a versão que você está usando.

O Citrix ADC é um controlador de entrega de aplicativos que analisa o tráfego específico do aplicativo para distribuir, otimizar e proteger de forma inteligente o tráfego de rede da Camada 4 à Camada 7 (L4–L7) para aplicativos web. O dispositivo virtual Citrix ADC VPX pode ser hospedado em várias plataformas de virtualização e nuvem. Para obter detalhes, consulte Implantar uma instância do Citrix ADC VPX.

SDKs e APIs

SDK PowerShell Remoto do Citrix DaaS™

O SDK PowerShell Remoto automatiza tarefas complexas e repetitivas. Ele fornece o mecanismo para configurar e gerenciar o ambiente do Citrix DaaS (anteriormente serviço Citrix Virtual Apps and Desktops™) sem usar o Studio.

- Os detalhes do cmdlet são fornecidos em SDK do Citrix DaaS.
- Os módulos suportados estão listados em Suporte e limitações. Essa seção também lista os cmdlets que estão desabilitados neste SDK.
- O SDK PowerShell Remoto está disponível para download no site da Citrix.

Este produto suporta as versões 3 a 7.6 do PowerShell.

Como este SDK difere do SDK para implantações gerenciadas pelo cliente

Em uma implantação do Citrix Virtual Apps and Desktops que é instalada e gerenciada por administradores do cliente, esses administradores executam cmdlets e scripts em um site contendo VDAs e Delivery Controllers dentro de uma estrutura de domínio comum. Em contraste, o Citrix DaaS divide os VDAs e os Controllers em um local de recurso e no plano de controle, respectivamente. Essa divisão significa que o SDK PowerShell original do Citrix Virtual Apps and Desktops não funciona em um ambiente Citrix DaaS. Ele não pode cruzar o limite seguro do local de recurso para o plano de controle.

A solução é o SDK PowerShell Remoto do Citrix DaaS. Ao ser executado no local de recurso, o SDK PowerShell Remoto acessa o plano de controle como se fosse local. Isso fornece a mesma funcionalidade de um único site do Citrix Virtual Apps and Desktops. Existe apenas a camada de comunicação não visível mais baixa, aprimorada para funcionar em um único site local ou no ambiente de nuvem. Os cmdlets são os mesmos, e a maioria dos scripts existentes permanece inalterada.

O cmdlet `Get-XdAuthentication` fornece a autorização para cruzar o limite seguro do local de recurso para o plano de controle. Por padrão, `Get-XdAuthentication` solicita aos usuários as credenciais CAS e deve ser feito uma vez por sessão do PowerShell. Alternativamente, o usuário pode definir um perfil de autenticação usando um Cliente Seguro de acesso à API, criado no

console do Citrix Cloud™. Em ambos os casos, as informações de segurança persistem para uso em chamadas subsequentes do SDK PowerShell. Se este cmdlet não for executado explicitamente, ele será chamado pelo primeiro cmdlet do SDK PowerShell.

Pré-requisitos

Para usar o SDK PowerShell Remoto do Citrix DaaS, adicione as seguintes URLs à lista de permissões:

Comercial

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

Japão

- `https://*.citrixcloud.jp`
- `https://*.citrixworkspacesapi.jp/[customerid]`
- `https://[customerid].apps.citrixworkspacesapi.jp:443`

Governo

- `hhttps://*.cloud.us`
- `https://*.citrixworkspacesapi.us/[customerid]`
- `https://[customerid].xendesktop.us:443`

Instalar e usar o SDK do PowerShell Remoto

Requisitos e considerações:

> **Observação:**

> Não instale o SDK do PowerShell Remoto em uma máquina Citrix Cloud Connector™. Ele pode ser instalado em qualquer máquina ingressada no domínio dentro do mesmo local de recurso.

> A Citrix® não oferece suporte à execução dos cmdlets deste SDK em Cloud Connectors. A operação do SDK não envolve os Cloud Connectors.

> Se você também tiver uma implantação do Citrix Virtual Apps and Desktops (além do Citrix DaaS), não instale o Remote PowerShell SDK em um Delivery Controller local. Como o Citrix Studio (baseado em MMC) é instalado como parte do Delivery Controller, você também não pode instalar o SDK em um servidor que esteja executando o Citrix Studio.

- Instale o **Microsoft Edge WebView2**.
- Certifique-se de que o PowerShell 3.0, 4.0, 5.0, 6.0 ou 7.0 esteja disponível na máquina.
- O instalador do SDK baixa e instala o .NET Framework 4.8 se ele (ou uma versão posterior compatível) ainda não estiver instalado.
- Se a máquina já tiver o Citrix Virtual Apps and Desktops SDK instalado, remova esse SDK (em Programas e Recursos do Windows) antes de instalar o Remote PowerShell SDK.
- Para um ambiente automatizado, use o parâmetro `-quiet` para instalar o SDK sem a intervenção do usuário.

Para instalar o Remote PowerShell SDK:

1. Na página de download, baixe o Virtual Apps and Desktops Remote PowerShell SDK.
2. Instale e execute o SDK.

Os logs de instalação são criados em `%TEMP%\CitrixLogs\CitrixPoshSdk`. Os logs podem ajudar a resolver problemas de instalação.

Execute o SDK em um computador ingressado no domínio dentro desse local de recurso:

- Abra um prompt de comando do PowerShell. Você não precisa executar como administrador.
- Se você quiser usar o snap-in (em vez do módulo), adicione o snap-in usando o cmdlet `Add-PSSnapin` (ou `asnp`).
- Você pode autenticar explicitamente usando o cmdlet `Get-XdAuthentication`. Alternativamente, execute seu primeiro comando do Remote PowerShell SDK, que solicitará a mesma autenticação que `Get-XdAuthentication`. Se você estiver usando um proxy, deverá autenticar no proxy para poder usar o cmdlet `Get-XdAuthentication`. Para obter mais informações, consulte Usar o Remote PowerShell SDK com um proxy.
- Para ignorar o prompt de autenticação, você pode usar o cmdlet `Set-XdCredentials` para criar um perfil de autenticação padrão, usando um Cliente Seguro criado no console do Citrix Cloud.

- Continue executando cmdlets do PowerShell SDK ou scripts de automação do PowerShell SDK. Veja um exemplo.

Para desinstalar o Remote PowerShell SDK, na funcionalidade do Windows para remover ou alterar programas, selecione **Citrix Virtual Apps and Desktops Remote PowerShell SDK**. Clique com o botão direito e selecione **Desinstalar**. Siga o diálogo.

Usar o Remote PowerShell SDK com um proxy

Se você estiver usando um proxy, talvez não consiga usar o cmdlet `Get-xdAuthentication` devido ao proxy bloquear as solicitações HTTP que o cmdlet faz.

Existem duas maneiras de autenticar no proxy. Você pode usar o parâmetro `ProxyUseDefault` ou os parâmetros `ProxyUsername` e `ProxyPassword`:

- O parâmetro `ProxyUseDefault` permite a autenticação no proxy usando as credenciais de proxy padrão. Por exemplo:

```
Get-XdAuthentication -ProxyUseDefault
```

- Os parâmetros `ProxyUsername` e `ProxyPassword` permitem a autenticação no proxy dentro da sessão do PowerShell. Por exemplo:

```
$secureString = ConvertTo-SecureString -String "password" -AsPlainText
-Force



Get-XdAuthentication -ProxyUsername user1 -ProxyPassword $secureString
```

Nota:

Você receberá um erro se executar um comando com `XDHyp:\` no Remote PowerShell SDK. Para resolver este problema:

1. Execute um comando com `Hyp`. Por exemplo: `Get-HypServiceStatus`

2. Execute um comando com `XDHyp:\`. Por exemplo: `Get-ChildItem XDHyp:\Connections\`

Exemplos de atividades

As atividades comuns incluem a configuração de catálogos de máquinas, aplicativos e usuários. Um script de exemplo é mostrado abaixo.

```
    $users = "xd.local\Domain Users"


    $TSVDACatalogName = "TSVDA"


    $TSVDADGName = "TSVDA"


    $TSVDAMachineName = "xd\ds-tsvda2"


    #Create TSVDA Catalog


    $brokerUsers = New-BrokerUser -Name $users


    $catalog = New-BrokerCatalog -Name $TSVDACatalogName -AllocationType
"Random" -Description $TSVDACatalogName -PersistUserChanges "OnLocal"
-ProvisioningType "Manual" -SessionSupport "MultiSession"
-MachinesArePhysical $true


    #Add TSVDA Machine to Catalog
```

```
    $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
-CatalogUid $catalog.uid



    #Create new desktops & applications delivery group



    $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
$TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession"
-DeliveryType DesktopsAndApps -Description $TSVDADGName



    #Create notepad application



    New-BrokerApplication -ApplicationType HostedOnDesktop -Name "Notepad"
-CommandLineExecutable "notepad.exe" -DesktopGroup $dg



    #Assign users to desktops and applications



    New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
$dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName



    New-BrokerAccessPolicyRule -Name $TSVDADGName
-IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers
-DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")



    New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
$dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName
```

```
#Add machine to delivery group



Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
```

Suporte e limitações

Os seguintes sistemas operacionais são suportados pelo Remote PowerShell SDK:

- Windows 11
- Windows 10
- Windows 10 IoT Enterprise LTSC x32 2019
- Windows 10 IoT Enterprise LTSC x64 2019
- Windows 10 IoT Enterprise 21h1 x64
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Os seguintes módulos PowerShell do Citrix Virtual Apps and Desktops são suportados nesta versão:

- Broker
- Identidade do Active Directory (AD)
- Criação de máquina
- Configuração
- Registro de configuração
- Host
- Administração delegada
- Análise

Para obter detalhes sobre cmdlets, consulte Citrix Virtual Apps and Desktops SDK.

Após a autenticação, o acesso remoto permanece válido na sessão atual do PowerShell por 24 horas. Após esse período, você deve inserir suas credenciais.

O SDK do Remote PowerShell deve ser executado em um computador dentro do local do recurso.

Os seguintes cmdlets são desabilitados em operações remotas para manter a integridade e a segurança do plano de controle do Citrix Cloud.

Citrix.ADIdentity.Admin.V2:

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection
- Set-AcctServiceMetadata
- Set-AcctADAccountUserCert
- Test-AcctDBConnection

Citrix.Analytics.Admin.V1:

- Get-AnalyticsDBConnection
- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite
- Set-AnalyticsDBConnection

Citrix.DelegatedAdmin.Admin.V1:

- Add-AdminRight
- Get-AdminDBConnection
- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminRight
- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator
- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminServiceMetadata
- Test-AdminDBConnection

Citrix.Broker.Admin.V2:

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- Get-BrokerController
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease
- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata

- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata
- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata
- Set-BrokerSiteMetadata
- Test-BrokerDBConnection
- Test-BrokerLicenseServer
- Update-BrokerBrokerLocalLeaseCache

Citrix.Configuration.Admin.V2:

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript
- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership

- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection
- Unregister-ConfigRegisteredServiceInstance

Citrix.Host.Admin.V2:

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript
- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership
- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

Citrix.ConfigurationLogging.Admin.V1:

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore
- Reset-LogServiceGroupMembership

- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

Citrix.MachineCreation.Admin.V2:

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata
- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceMetadata
- Test-ProvDBConnection

Citrix.EnvTest.Admin.V1:

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership
- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

Citrix.Monitor.Admin.V1:

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata
- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

Citrix.Storefront.Admin.V1:

- Build-SfCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

Módulo de descoberta do Citrix DaaS para pacotes e servidores App-V

O Citrix DaaS pode entregar aplicativos contidos em pacotes App-V aos seus endpoints usando um dos seguintes métodos:

- Método de gerenciamento de administrador único (acessando pacotes de um compartilhamento de rede)
- Método de gerenciamento de administrador duplo (acessando pacotes de um Servidor de Gerenciamento Microsoft App-V)

O processo de registro de pacotes App-V, Gerenciamento Microsoft App-V e Servidores de Publicação com a Biblioteca de Aplicativos usando o Citrix DaaS difere ligeiramente do registro de pacotes usando uma implantação local. No entanto, o processo de atribuição de aplicativos aos usuários e seu lançamento no endpoint de um usuário é idêntico.

O console de gerenciamento do Citrix DaaS no Citrix Cloud não pode visualizar arquivos em um local de recurso. Além disso, ele não pode descobrir diretamente pacotes App-V ou servidores Microsoft App-V em sua infraestrutura. O módulo de descoberta fornece funções que descobrem informações de pacotes App-V em sua infraestrutura local e as carrega para o seu Citrix DaaS. As informações do pacote incluem pacotes App-V, servidores Microsoft App-V e os aplicativos que os pacotes contêm.

O módulo de descoberta usa o SDK do PowerShell Remoto do Virtual Apps and Desktops. Ele pode descobrir informações de pacotes de um compartilhamento de rede ou de um Servidor de Gerenciamento Microsoft App-V. Você usa o módulo de descoberta em uma máquina em seu local de recurso.

Pré-requisitos para usar o módulo de descoberta:

- Verifique se o PowerShell 3.0 ou posterior está disponível na máquina.
- Verifique se o SDK do PowerShell Remoto do Citrix Virtual Apps and Desktops está instalado na máquina.
- Verifique se você tem acesso ao compartilhamento de rede que contém os pacotes App-V.
- Verifique se você tem acesso ao servidor onde os Citrix Cloud Connectors estão instalados e onde o Servidor de Gerenciamento Microsoft App-V está hospedado.

Adicionar pacotes App-V à Biblioteca de Aplicativos no Citrix Cloud

O procedimento a seguir é válido para adicionar pacotes App-V de compartilhamentos de rede (gerenciamento de administrador único) e adicionar todos os pacotes App-V publicados do Microsoft App-V Management Server (gerenciamento de administrador duplo). Com o método de gerenciamento de administrador duplo, você deve gerenciar os pacotes App-V adicionados da mesma forma que faria ao usar o método de gerenciamento de administrador único.

1. Baixe o módulo de descoberta na página de downloads do Citrix DaaS `<https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html>`. Extraia o arquivo zip `Citrix.Cloud.AppLibrary.Admin.v1.psm1` para uma pasta conveniente.

> **Nota:**
>
> Este arquivo também é fornecido na ISO do Citrix Virtual Apps and Desktops em `Support\Tools\Scripts`. Você pode copiá-lo localmente ou referenciá-lo diretamente da unidade de CD.

2. Verifique se o SDK do PowerShell Remoto do Virtual Apps and Desktops está instalado em sua máquina
3. navegar para a pasta que contém o módulo de descoberta. Na janela do PowerShell, digite o caminho completo da pasta que contém o módulo de descoberta e pressione **Enter**.
4. Importe o módulo de descoberta com o comando `Import-Module. \Citrix.Cloud.AppLibrary.Admin.v1.psm1`.
5. Adicione os pacotes App-V à Biblioteca de Aplicativos no Citrix Cloud usando um dos seguintes métodos.

   - Para adicionar pacotes App-V de um compartilhamento de rede, execute o cmdlet do PowerShell: `Import-AppVPackageToCloud`.

     Por exemplo: `Import-AppVPackageToCloud –PackagePath \ \AppVSrv\share\Notepad++.appv`

     Para obter ajuda sobre o cmdlet, digite `Get-Help Import-AppVPackageToCloud`.
   - Para adicionar pacotes App-V de um Microsoft App-V Management Server, execute o cmdlet do PowerShell: `Import-AppVPackagesFromManagementServerToCloud`

     Por exemplo: `Import-AppVPackagesFromManagementServerToCloud –ManagementSrvFQDN AppVMngSrv.domain.local`

     Para obter ajuda sobre o cmdlet, digite `Get-Help Import-AppVPackagesFromManagementServerToCloud`

     Este comando importa todos os pacotes App-V publicados do Microsoft App-V Management Server para o Citrix Cloud.

     Depois de adicionar os pacotes App-V ao Citrix Cloud, você deve gerenciá-los como faria usando o método de gerenciamento de administrador único.
6. Faça login no Citrix Cloud. Selecione o cliente de destino. Após a execução bem-sucedida do script, os pacotes App-V são adicionados à Biblioteca de Aplicativos no Citrix Cloud.

Funções PowerShell de alto nível

O módulo contém as seguintes funções de alto nível que você pode chamar do seu próprio script PowerShell:

- `Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>`

  Descobre e carrega para o Citrix DaaS todas as informações necessárias para publicar aplicativos de um único Pacote App-V.

- `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>`

  Descobre os caminhos UNC de pacotes publicados pelo Servidor de Gerenciamento e chama **Import-AppVPackageToCloud** para cada um, por sua vez.

  Os pacotes descobertos dessa forma são carregados para o Citrix DaaS usando o método de gerenciamento de administrador único. O Citrix DaaS não pode entregar pacotes usando o método de gerenciamento de administrador duplo.

- `Import-AppVDualAdminToCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Descobre Servidores de Gerenciamento e Publicação do Microsoft App-V e importa o conteúdo para a Biblioteca de Aplicativos. Este cmdlet importa todos os pacotes gerenciados usando o Servidor de Gerenciamento do Microsoft App-V e informações relacionadas. Os servidores podem ser adicionados e removidos via PowerShell.

  Este cmdlet adiciona pacotes App-V no modo de administrador duplo. Apenas pacotes App-V que são publicados no Servidor de Gerenciamento do Microsoft App-V e que têm grupos AD adicionados são importados. Se você fizer alterações no Servidor de Gerenciamento do Microsoft App-V, execute novamente este cmdlet para sincronizar a Biblioteca de Aplicativos com o Servidor de Gerenciamento do Microsoft App-V.

- `Remove-AppVServerFromCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Remove os Servidores de Gerenciamento e Publicação do Microsoft App-V adicionados à Biblioteca de Aplicativos.

Este cmdlet remove os Servidores de Gerenciamento e Publicação do Microsoft App-V especificados, além de todos os pacotes App-V associados.

Execute o módulo de descoberta para pacotes e servidores App-V em um computador ingressado no domínio dentro desse local de recurso. Siga as orientações em Instalar e usar o SDK do PowerShell Remoto para começar. Continue executando cmdlets ou scripts do PowerShell. Veja os exemplos a seguir.

Atividades de exemplo

Importe o módulo de descoberta de pacotes App-V do Citrix DaaS.

```
import-module "D:
\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

Percorra o diretório da loja de pacotes App-V e carregue cada pacote.

```
Get-ChildItem -Path "\\FileServer.domain.net\App-V Packages" -Filter
*.appv |

Foreach-Object{

    Import-AppVPackageToCloud -PackagePath $_.FullName

}
```

Descubra e carregue pacotes registrados em um servidor de gerenciamento Microsoft App-V.

```
Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN
AppVManagementServer.domain.net
```

Descubra os Servidores de Gerenciamento e Publicação do Microsoft App-V e adicione a configuração à Biblioteca de Aplicativos. Isso também importa todos os pacotes gerenciados pelo Servidor de Gerenciamento do Microsoft App-V no modo de administração dupla.

```
Import-AppVDualAdminCloud -ManagementSrvUrl http://
AppVManagementServer.domain.net –PublishingServerUrl http://
AppVManagementServer.domain.net:8001
```

Leia a documentação de ajuda do PowerShell incluída no módulo.

```
Get-Help Import-AppVPackageToCloud
```

Limitações

- Você não pode descobrir pacotes App-V em sua infraestrutura de local de recurso diretamente do console de gerenciamento do Citrix DaaS no Citrix Cloud. Para obter mais informações sobre o Citrix Cloud, consulte a documentação do Citrix Cloud.
- O console de gerenciamento do Citrix DaaS no Citrix Cloud não tem uma conexão ativa com o servidor de gerenciamento do Microsoft App-V. As alterações em Pacotes e outras configurações no servidor de gerenciamento do Microsoft App-V não são refletidas no console de gerenciamento do Citrix DaaS até que `Import-AppVDualAdminCloud` seja executado novamente.

API OData do Serviço de Monitoramento

Além de usar as funções de Monitoramento para exibir dados históricos, você pode consultar dados usando a API do Serviço de Monitoramento. Use a API para:

- Analisar tendências históricas para planejamento
- Realizar solução de problemas detalhada de falhas de conexão e máquina
- Extrair informações para alimentar outras ferramentas e processos; por exemplo, usando tabelas PowerPivot do Microsoft Excel para exibir os dados de diferentes maneiras
- Construir uma interface de usuário personalizada com base nos dados fornecidos pela API

Para obter detalhes, consulte Monitor Service OData API. Para acessar a API do Monitor Service, consulte Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

APIs do Citrix DaaS

Para obter uma lista abrangente das APIs do Citrix DaaS, consulte Citrix DaaS APIs.

Aviso legal

Este software / código de exemplo é fornecido a você "COMO ESTÁ", sem representações, garantias ou condições de qualquer tipo. Você pode usá-lo, modificá-lo e distribuí-lo por sua própria conta e risco. A CITRIX SE ISENTA DE TODAS E QUAISQUER GARANTIAS, EXPRESSAS, IMPLÍCITAS, ESCRITAS, ORAIS OU ESTATUTÁRIAS, INCLUINDO, SEM LIMITAÇÃO, GARANTIAS DE COMERCIABILIDADE, ADEQUAÇÃO A UMA FINALIDADE

ESPECÍFICA, TÍTULO E NÃO VIOLAÇÃO. Sem limitar a generalidade do exposto, você reconhece e concorda que (a) o software / código de exemplo pode apresentar erros, falhas de design ou outros problemas, possivelmente resultando em perda de dados ou danos à propriedade; (b) pode não ser possível tornar o software / código de exemplo totalmente funcional; e (c) a Citrix pode, sem aviso prévio ou responsabilidade para com você, deixar de disponibilizar a versão atual e/ou quaisquer versões futuras do software / código de exemplo. Em nenhuma hipótese o software / código deve ser usado para apoiar atividades de alto risco, incluindo, mas não se limitando a, suporte à vida ou atividades de detonação. NEM A CITRIX NEM SUAS AFILIADAS OU AGENTES SERÃO RESPONSÁVEIS, SOB VIOLAÇÃO DE CONTRATO OU QUALQUER OUTRA TEORIA DE RESPONSABILIDADE, POR QUAISQUER DANOS DECORRENTES DO USO DO SOFTWARE / CÓDIGO DE EXEMPLO, INCLUINDO, SEM LIMITAÇÃO, DANOS DIRETOS, ESPECIAIS, INCIDENTAIS, PUNITIVOS, CONSEQUENCIAIS OU OUTROS DANOS, MESMO QUE AVISADOS DA POSSIBILIDADE DE TAIS DANOS. Você concorda em indenizar e defender a Citrix contra quaisquer reivindicações decorrentes do seu uso, modificação ou distribuição do código.

index

- Conexão com o Citrix Hypervisor
- Criar um catálogo do Citrix Hypervisor
- Gerenciar um catálogo do Citrix Hypervisor
- Solução de problemas no Quick Deploy
- Usuários e autenticação no Quick Deploy
- Assinaturas do Azure no Quick Deploy
- Criar catálogos usando o Quick Deploy
- Gerenciar catálogos no Quick Deploy
- Introdução ao Quick Deploy
- Imagens no Quick Deploy
- Monitorar no Quick Deploy
- Conexões de rede no Quick Deploy
- Referência ao Quick Deploy
- Acesso remoto ao PC no Quick Deploy
- Solução de problemas no Quick Deploy
- Usuários e autenticação no Quick Deploy
- Migrar a configuração para o Citrix Cloud
- Cmdlets da ferramenta de configuração automatizada
- Solucionar problemas de configuração automatizada e informações adicionais
- Migração da nuvem para a nuvem
- Migração do local para a nuvem
- Mesclar vários sites em um único site

Conexão com o Citrix Hypervisor

Create and manage connections descreve os assistentes que criam uma conexão. As informações a seguir abrangem detalhes específicos dos ambientes de virtualização do Citrix Hypervisor.

> **Nota:**
>
> Antes de criar uma conexão com o Citrix Hypervisor, você precisa primeiro concluir a configuração da sua conta do Citrix Hypervisor como um local de recursos. Consulte Ambientes de virtualização do Citrix Hypervisor.

Criar uma conexão ao Citrix Hypervisor

Ao criar uma conexão com o Citrix Hypervisor (anteriormente XenServer), você deve fornecer as credenciais para um usuário VM Power Admin ou de nível superior.

A Citrix recomenda o uso de HTTPS para proteger as comunicações com o Citrix Hypervisor. Para usar HTTPS, você deve substituir o certificado TLS padrão instalado no Citrix Hypervisor. Para obter mais informações, consulte Instalar um certificado TLS no seu servidor.

Você pode configurar a alta disponibilidade se ela estiver ativada no servidor Citrix Hypervisor. A Citrix recomenda que você selecione todos os servidores no pool (em **Edit High Availability**) para permitir a comunicação com o servidor Citrix Hypervisor se o mestre do pool falhar.

> **Nota:**
>
> Se você estiver usando HTTPS e quiser configurar servidores de alta disponibilidade, não instale um certificado curinga para todos os servidores em um pool. É necessário um certificado individual para cada servidor.

> Você pode selecionar um tipo e um grupo de GPU, ou Passthrough, se o Citrix Hypervisor oferecer suporte a vGPU. A exibição indica se a seleção possui recursos de GPU dedicados.

Ao usar o armazenamento local em um ou mais hosts Citrix Hypervisor para armazenamento de dados temporário, certifique-se de que cada local de armazenamento no pool tenha um nome exclusivo. (Para alterar um nome no XenCenter, clique com o botão direito do mouse no armazenamento e edite a propriedade do nome.)

Usar o IntelliCache para conexões do Citrix Hypervisor

Usando o IntelliCache, as implantações de VDI hospedadas são mais econômicas porque você pode usar uma combinação de armazenamento compartilhado e armazenamento local. Isso

melhora o desempenho e reduz o tráfego de rede. O armazenamento local armazena em cache a imagem mestre do armazenamento compartilhado, o que reduz o número de leituras no armazenamento compartilhado. Para áreas de trabalho compartilhadas, as gravações nos discos diferenciais são gravadas no armazenamento local no host e não no armazenamento compartilhado.

- O armazenamento compartilhado deve ser NFS quando usar o IntelliCache.
- A Citrix recomenda que você use um dispositivo de armazenamento local de alto desempenho para garantir a transferência de dados mais rápida possível.

Para usar o IntelliCache, você deve ativá-lo no produto e no Citrix Hypervisor.

- Quando instalar o Citrix Hypervisor, selecione **Enable thin provisioning (Optimized storage for Citrix Virtual Desktops)**. O Citrix não oferece suporte a pools mistos de servidores que têm o IntelliCache ativado e os que não têm. Para obter mais informações, consulte a documentação do Citrix Hypervisor.
- No Citrix Virtual Apps and Desktops, o IntelliCache é desativado por padrão. Você pode alterar a configuração somente ao criar uma conexão Citrix Hypervisor; não é possível desativar o IntelliCache posteriormente. Quando você adiciona uma conexão Citrix Hypervisor:
  - Selecione **Shared** como o tipo de armazenamento.
  - Selecione a caixa de seleção **Use IntelliCache**.

O que fazer a seguir

- Se você estiver no processo de implantação inicial, consulte Criar catálogos de máquinas.
- Para obter informações específicas do Citrix Hypervisor, consulte Criar um catálogo do Citrix Hypervisor.

Mais informações

- Conexões e recursos
- Ambientes de virtualização do Citrix Hypervisor

Criar um catálogo do Citrix Hypervisor

Criar catálogos de máquinas descreve os assistentes que criam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes de virtualização do Citrix Hypervisor.

> **Nota:**
>
> Antes de criar um catálogo do Citrix Hypervisor, você precisa concluir a criação de uma conexão com o Citrix Hypervisor. Consulte Conexão com o Citrix Hypervisor.

Criar um catálogo de máquina usando uma conexão do Citrix Hypervisor

As máquinas com capacidade para GPU exigem uma imagem mestre dedicada. Essas VMs exigem drivers de placa de vídeo que suportem GPUs. Configure máquinas compatíveis com GPU para permitir que a VM opere com o software que usa a GPU para operações.

1. No XenCenter, crie uma VM com VGA padrão, redes e vCPU.
2. Atualize a configuração da VM para habilitar o uso de GPU (Passthrough ou vGPU).
3. Instale um sistema operacional suportado e ative o RDP.
4. Instale os drivers Citrix VM Tools e NVIDIA.
5. Desative o console de administração do Virtual Network Computing (VNC) para otimizar o desempenho e reinicie a VM.
6. Você será solicitado a usar o RDP. Usando o RDP, instale o VDA e reinicialize a VM.
7. Opcionalmente, crie um instantâneo para a VM como um modelo de linha de base para outras imagens mestre de GPU.
8. Usando o RDP, instale aplicativos específicos do cliente configurados no XenCenter e use recursos de GPU.

Criar um catálogo de máquinas usando um perfil de máquina

Ao criar um catálogo para provisionar máquinas usando o MCS, você pode usar um perfil de máquina para capturar as propriedades de hardware de uma máquina virtual e aplicá-las às VMs recém-provisionadas no catálogo. Se o parâmetro `MachineProfile` não for usado, as propriedades do hardware são capturadas da VM da imagem mestre ou do instantâneo.

> **Nota:**
>
> Atualmente, você pode usar somente uma VM como entrada de perfil de máquina.

> Você pode configurar explicitamente os seguintes parâmetros para substituir os valores dos parâmetros na entrada do perfil da máquina:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

Para criar um catálogo com um perfil de máquina:

1. Abra uma janela do PowerShell.
2. Execute `asnp citrix*`.
3. Crie um pool de identidades. O pool de identidades é um contêiner para as contas do Active Directory (AD) das VMs a serem criadas. Por exemplo:

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
"ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
"Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. Crie as contas de computador do AD necessárias no Active Directory.

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -Force

New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count 10
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. Execute o comando `New-ProvScheme` para criar um catálogo. Por exemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
```

```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. Registre o esquema de provisionamento como um catálogo de agente. Por exemplo:

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. Adicione VMs ao catálogo de máquinas.

Para atualizar um catálogo com um novo perfil de máquina:

1. Execute o comando `Set-ProvScheme`. Por exemplo:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

Para obter mais informações sobre o comando Set-ProvScheme, consulte Set-ProvScheme.

Nota:

- Nesse caso, o comando `Set-ProvScheme` não altera o perfil da máquina das VMs existentes no catálogo. Somente as VMs recém-criadas adicionadas ao catálogo têm o novo perfil de máquina.
- Não é possível converter um catálogo de máquinas baseado em perfil de máquina em um catálogo de máquinas não baseado em perfil de máquina.

O que fazer a seguir

- Se este for o primeiro catálogo criado, você será guiado para criar um grupo de entrega.
- Para revisar todo o processo de configuração, consulte Planejar e criar uma implantação.
- Para gerenciar catálogos, consulte Gerenciar catálogos de máquinas e Gerenciar um catálogo do Citrix Hypervisor.

Mais informações

- Conexões e recursos
- Conexão com o Citrix Hypervisor
- Criar catálogos de máquinas

Gerenciar um catálogo do Citrix Hypervisor

Gerenciar catálogos de máquinas descreve os assistentes que gerenciam um catálogo de máquinas. As informações a seguir abrangem detalhes específicos dos ambientes de virtualização do Citrix Hypervisor.

Nota:

Antes de gerenciar um catálogo do Citrix Hypervisor, você precisa concluir a criação de um catálogo do Citrix Hypervisor. Consulte Criar um catálogo do Citrix Hypervisor.

Identificar recursos criados pelo MCS

A seguir estão as tags que o MCS adiciona aos recursos na plataforma Citrix Hypervisor. As tags na tabela são representadas como "key":"value".

NOME DO RECURSO	MARCA
Cópia do disco em cada rede ou armazenamento local (somente no local)	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco de identificação	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco do sistema operacional	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"
Disco básico publicado	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM in catalog	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"
Disco WBC	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Mais informações

- Conexões e recursos
- Conexão com o Citrix Hypervisor
- Criar catálogos de máquinas
- Criar um catálogo do Citrix Hypervisor
- Gerenciar catálogos de máquinas

Solução de problemas no Quick Deploy

Introdução

Os locais de recursos contêm as máquinas que fornecem áreas de trabalho e aplicativos. Essas máquinas são criadas em catálogos, portanto, os catálogos são considerados parte do local de recursos. Cada local de recursos também contém Cloud Connectors. Os Cloud Connectors permitem que o Citrix Cloud se comunique com o local do recurso. Normalmente, a Citrix instala e atualiza os Cloud Connectors.

Opcionalmente, você pode iniciar vários Cloud Connector e ações de localização de recursos. Veja:

- Ações nos locais de recursos
- Configurações de localização de recursos ao criar um catálogo

O Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) tem ferramentas para solução de problemas e suporte que podem ajudar a resolver problemas de configuração e comunicação com as máquinas que fornecem áreas de trabalho e aplicativos (os VDAs). Por exemplo, a criação de um catálogo pode falhar ou os usuários podem não conseguir iniciar a área de trabalho ou os aplicativos.

Essa solução de problemas inclui obter acesso à sua assinatura do Citrix Managed Azure por meio de uma máquina bastion ou RDP direto. Depois de obter acesso à assinatura, você pode usar as ferramentas de suporte da Citrix para localizar e resolver problemas. Para obter detalhes, consulte:

- Solução de problemas de VDA usando um bastion ou RDP direto
- Acesso ao bastion
- Acesso direto ao RDP

Solução de problemas de VDA usando um bastion ou RDP direto

Os recursos de suporte são para pessoas com experiência na solução de problemas da Citrix. Isso inclui:

- Citrix Service Providers (CSP) e outros que tenham conhecimento técnico e experiência em solução de problemas com os produtos Citrix DaaS.
- Equipe de suporte Citrix.

Se não estiver familiarizado ou não se sentir seguro para desempenhar a solução de problemas de componentes Citrix, você pode solicitar ajuda do Suporte Citrix. Os representantes do Suporte Citrix podem solicitar que você configure um dos métodos de acesso descritos nesta seção. No entanto, os representantes da Citrix desempenham a real solução do problema, usando as ferramentas e tecnologias Citrix.

> **Importante:**
>
> Esses recursos de suporte são válidos somente para máquinas ingressadas no domínio. Se as máquinas em seus catálogos não tiverem ingressadas no domínio, você será orientado a solicitar ajuda para a solução do problema ao Suporte Citrix.

Métodos de acesso

Estes métodos de acesso são válidos somente para a assinatura do Citrix Managed Azure. Para obter mais informações, consulte Assinaturas do Azure.

Dois métodos de acesso de suporte são fornecidos.

- Acesse seus recursos por meio de uma máquina bastion na assinatura dedicada do Citrix Managed Azure do cliente. O bastion é um ponto de entrada único que permite o acesso às máquinas na assinatura. Ele fornece uma conexão segura com esses recursos, permitindo o tráfego remoto de endereços IP em um intervalo especificado.

  As etapas desse método incluem:

  - Criar a máquina bastion
  - Baixar um agente RDP
  - Fazer RDP para a máquina bastion
  - Conectar-se da máquina bastion às outras máquinas Citrix em sua assinatura

  A máquina bastion é destinada ao uso de curto prazo. Esse método é destinado a problemas que envolvem a criação de catálogos ou máquinas de imagem.
- Acesso RDP direto às máquinas na assinatura dedicada do Citrix Managed Azure do cliente. Para permitir o tráfego RDP, a porta 3389 deve ser definida no grupo de segurança de rede.

  Esse método destina-se a problemas de catálogo não referentes a criação, como usuários que não conseguem iniciar suas áreas de trabalho.

Lembre-se: como alternativa a esses dois métodos de acesso, entre em contato com o Suporte Citrix para obter ajuda.

Acesso ao bastion

1. Em **Manage > Quick Deploy**, expanda **Troubleshoot & Support** à direita.
2. Clique em **View troubleshooting options**.
3. Na página **Troubleshoot**, selecione um dos dois primeiros tipos de problema e clique em **Use our troubleshooting machine**.
4. Na página **Troubleshoot with Bastion Machine**, selecione o catálogo.
    - Se as máquinas no catálogo selecionado não estiverem ingressadas no domínio, você será instruído a entrar em contato com o Suporte Citrix.
    - Se uma máquina bastion já tiver sido criada com acesso RDP à conexão de rede do catálogo selecionado, pule para a etapa 8.
5. O intervalo de acesso RDP é exibido. Se desejar restringir o acesso RDP a um intervalo menor do que o permitido pela conexão de rede, marque a caixa de seleção **Restrict RDP access to only computers in IP address range** e insira o intervalo desejado.
6. Digite o nome de usuário e senha que você usará para fazer login quando fizer RDP na máquina bastion. Requisitos de senha.

    Não use caracteres Unicode no nome de usuário.
7. Clique em **Create Bastion Machine**.

    Quando a máquina bastion é criada com sucesso, o título da página muda para **Bastion — *conexão***.

    Se a criação da máquina bastion falhar (ou se falhar durante a operação), clique em **Delete** na parte inferior da página de notificação da falha. Tente criar a máquina bastion novamente.

    Você pode alterar a restrição de alcance RDP depois que a máquina bastion for criada. Clique em **Edit**. Insira o novo valor e clique na marca de seleção para salvar a alteração. (Clique no **X** para cancelar a alteração.)
8. Clique em **Download RDP File**.
9. Faça o RDP para o bastion usando as credenciais que você especificou ao criar o bastion. (O endereço da máquina bastion é incorporado ao arquivo RDP que você baixou.)

10. Conecte-se da máquina bastion às outras máquinas Citrix na assinatura. Assim, você pode coletar logs e executar diagnósticos.

As máquinas bastion são ligadas quando são criadas. Para economizar custos, as máquinas são desligadas automaticamente se permanecerem ociosas após a inicialização. As máquinas são excluídas automaticamente após várias horas.

Você pode gerenciar a energia de uma máquina bastion ou excluí-la usando os botões na parte inferior da página. Se você optar por excluir uma máquina bastion, deve confirmar que sabe que todas as sessões ativas na máquina terminarão automaticamente. Além disso, que também todos os dados e arquivos salvos na máquina serão excluídos.

Acesso direto ao RDP

1. Em **Manage > Quick Deploy**, expanda **Troubleshoot & Support** à direita.
2. Clique em **View troubleshooting options**.
3. Na página **Troubleshoot**, selecione **Other catalog issue**.
4. Na página **Troubleshoot with RDP Access**, selecione o catálogo.

   Se o RDP já tiver sido habilitado para a conexão de rede do catálogo selecionado, pule para a etapa 7.
5. O intervalo de acesso RDP é exibido. Se desejar restringir o acesso RDP a um intervalo menor do que o permitido pela conexão de rede, marque a caixa de seleção **Restrict RDP access to only computers in IP address range** e insira o intervalo desejado.
6. Clique em **Enable RDP Access.**

   Quando o acesso RDP é ativado com êxito, o título da página muda para **RDP Access — *conexão***.

   Se o acesso RDP não for habilitado com êxito, clique em **Retry Enabling RDP** na parte inferior da página de notificação da falha.
7. Conecte-se às máquinas usando suas credenciais de administrador do Active Directory. Assim, você pode coletar logs e executar diagnósticos.

Obtenha ajuda

Se você ainda tiver problemas, abra um tíquete seguindo as instruções em Como obter ajuda e suporte.

Usuários e autenticação no Quick Deploy

Métodos de autenticação do usuário

Os usuários devem se autenticar ao fazer login no Citrix Workspace para iniciar suas áreas de trabalho ou aplicativos.

O Quick Deploy suporta os seguintes métodos de autenticação do usuário:

- **Managed Azure AD:** Managed Azure AD é um Azure Active Directory (AAD) fornecido e gerenciado pela Citrix. Você não precisa fornecer sua própria estrutura do Active Directory. Basta adicionar seus usuários ao diretório.
- **Seu provedor de identidade:** você pode usar qualquer método de autenticação disponível no Citrix Cloud.

> **Nota:**
>
> - As implantações do Remote PC Access usam somente o Active Directory. Para obter detalhes, consulte Remote PC Access.
> - Se você usa o Azure AD Domain Services: os UPNs de logon do Workspace devem conter o nome de domínio que foi especificado ao habilitar o Azure AD Domain Services. Logons não podem usar UPNs em domínios que você personaliza, mesmo que o domínio personalizado seja designado como primário.

A configuração da autenticação do usuário inclui os seguintes procedimentos:

1. Configure o método de autenticação do usuário no Citrix Cloud e Workspace Configuration.
2. Se você estiver usando o Managed Azure AD para autenticação de usuário, adicione usuários ao diretório.
3. Adicione usuários a um catálogo.

Configurar a autenticação do usuário no Citrix Cloud

Para configurar a autenticação do usuário no Citrix Cloud:

- Conecte-se ao método de autenticação do usuário que deseja usar. (No Citrix Cloud, você se “conecta” ou “desconecta” de um método de autenticação.)
- No Citrix Cloud, defina a autenticação do espaço de trabalho para usar o método conectado.

Nota:

O método de autenticação Managed Azure AD é configurado por padrão. Ou seja, ele é conectado automaticamente no Citrix Cloud, e a autenticação do Workspace é definida automaticamente para usar o Managed Azure AD for Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). Se você quiser usar esse método (e não tiver configurado um método diferente anteriormente), continue com Adicionar e excluir usuários no Managed Azure AD. Se o Managed Azure AD for desconectado, a autenticação do Workspace será transferida para o Active Directory. Se você quiser usar um método de autenticação diferente, siga as etapas abaixo.

Para alterar o método de autenticação:

1. Em **Manage > Quick Deploy**, selecione **User Access & Authentication** à direita.

2. Selecione **Manage User Access and Authentication**. Selecione a guia **Workspace**, se ainda não estiver selecionada. (A outra guia indica qual método de autenticação de usuário está configurado no momento.)

3. Siga o link **To set up authentication methods**. O link leva você ao Citrix Cloud. No menu de reticências, selecione **Connect** para o método desejado.
4. Enquanto ainda estiver no Citrix Cloud, selecione **Workspace Configuration** no menu superior esquerdo. Na guia **Authentication**, selecione o método desejado.

O que fazer a seguir:

- Se estiver usando o Managed Azure AD, adicione usuários ao diretório.
- Para todos os métodos de autenticação, adicione usuários ao catálogo.

Adicionar e excluir usuários no Managed Azure AD

Siga este procedimento somente se estiver usando o Managed Azure AD para autenticação do usuário no Citrix Workspace.

Você fornece o nome e o endereço de e-mail de seus usuários. Em seguida, a Citrix envia um convite por e-mail para cada um deles. O e-mail instrui os usuários a selecionar um link que os ingresse no Citrix Managed Azure AD.

- Se o usuário já tiver uma conta da Microsoft com o endereço de e-mail fornecido, essa conta será usada.
- Se o usuário não tiver uma conta da Microsoft com o endereço de e-mail, a Microsoft criará uma conta.

Para adicionar e convidar usuários para o Managed Azure AD:

1. Em **Manage > Quick Deploy**, expanda **User Access & Authentication** à direita. Selecione **Manage User Access and Authentication**.
2. Selecione a guia **Managed Azure AD**.
3. Selecione **Invite Users**.

   
4. Digite o nome e o endereço de e-mail de um usuário e selecione **Add User**.

   
5. Repita a etapa anterior para adicionar outros usuários.
6. Quando terminar de adicionar as informações do usuário, selecione **Invite Users** na parte inferior do cartão.

Para excluir um usuário do Managed Azure AD, selecione o ícone de lixeira ao lado do nome do usuário que deseja excluir do diretório. Confirme a exclusão.

O que fazer a seguir: Adicionar usuários ao catálogo

Adicionar ou remover usuários em um catálogo

Conclua este procedimento independentemente do método de autenticação usado.

1. Em **Manage > Quick Deploy**, se você não adicionou nenhum usuário a um catálogo, selecione **Add subscribers**.

   Para adicionar usuários a um catálogo que já tem usuários, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Subscribers**, selecione **Manage Subscribers**.



3. Selecione um domínio. (Se você estiver usando o Managed Azure AD para autenticação de usuário, há apenas uma entrada no campo de domínio.) Em seguida, selecione um usuário.



4. Selecione outros usuários, conforme necessário. Quando terminar, selecione o **X** no canto superior direito.

Para remover usuários de um catálogo, siga as etapas 1 e 2. Na etapa 3, selecione o ícone de lixeira ao lado do nome que deseja excluir (em vez de selecionar um domínio e grupo/usuário). Essa ação remove o usuário do catálogo, não da origem (como o Managed Azure AD ou o seu próprio AD ou AAD).

O que fazer a seguir:

- Para um catálogo com máquinas multissessão, adicione aplicativos, se ainda não o fez.
- Para todos os catálogos, envie a URL do Citrix Workspace para os seus usuários.

Mais informações

Para obter mais informações sobre autenticação no Citrix Cloud, consulte Gerenciamento de identidade e acesso.

Assinaturas do Azure no Quick Deploy

Introdução

Ao criar um catálogo ou criar uma imagem no Quick Deploy, você escolhe entre as assinaturas do Azure disponíveis. O Quick Deploy é compatível com assinaturas do Citrix Managed Azure e suas próprias assinaturas do Azure gerenciadas pelo cliente.

- Para usar sua própria assinatura do Azure, primeiro importe (adicione) uma ou mais dessas assinaturas para o Citrix DaaS (antigo serviço Citrix Virtual Apps and Desktops). Essa ação permite que o Citrix DaaS acesse suas assinaturas do Azure.
- O uso de uma assinatura do Citrix Managed Azure não requer configuração de assinatura. No entanto, uma assinatura do Citrix Managed Azure está disponível somente quando você solicita o Citrix Azure Consumption Fund, além do Citrix DaaS.

Alguns recursos do Citrix DaaS diferem, dependendo de o catálogo usar uma assinatura do Citrix Managed Azure ou estar em sua própria assinatura do Azure.

ASSINATURA DO CITRIX MANAGED AZURE	SUA PRÓPRIA ASSINATURA DO AZURE
Oferece suporte a máquinas ingressadas no domínio ou não ingressadas no domínio.	Oferece suporte somente a máquinas ingressadas no domínio.
Oferece suporte à criação rápida e criação personalizada de catálogos.	Oferece suporte apenas a catálogos criados pelo usuário.
Sempre disponível ao criar catálogos e imagens.	É necessário adicionar a assinatura do Azure ao Citrix DaaS antes de criar um catálogo.
Para autenticação do usuário, é compatível com o Citrix Managed Azure Active Directory ou seu próprio Active Directory.	Pode conectar seu próprio Active Directory e Azure Active Directory.
As opções de conexão de rede incluem **No connectivity**.	As opções de conexão de rede incluem apenas suas próprias redes virtuais.
Ao usar o emparelhamento de VNet do Azure para se conectar aos seus recursos, você deve criar uma conexão de mesmo nível VNet no Citrix DaaS.	Selecione uma rede virtual existente.
Ao importar uma imagem do Azure, você especifica o URI da imagem.	Ao importar uma imagem, você pode selecionar um VHD ou navegar pelo armazenamento na assinatura do Azure.
Pode criar uma máquina bastion assinatura do Azure do cliente para solucionar problemas de máquinas.	Não é necessário criar uma máquina bastion porque você já pode acessar as máquinas em sua assinatura.

Veja as assinaturas do Azure

Para visualizar os detalhes da assinatura do Azure, em **Manage > Quick Deploy**, expanda **Cloud Subscriptions** à direita. Em seguida, selecione uma entrada de assinatura.

- A página **Details** contém o número de máquinas, além dos números e nomes de catálogos e imagens que usam a assinatura.
- A página **Resource Locations** lista os locais de recursos em que a assinatura é usada.

Adicionar assinaturas do Azure gerenciadas pelo cliente

Para usar uma assinatura do Azure gerenciada pelo cliente, você deve adicioná-la ao Citrix DaaS antes de criar um catálogo ou criar uma imagem que use essa assinatura. Você tem duas opções ao adicionar suas assinaturas do Azure:

- **Se você for um Administrador Global do diretório e tiver permissões de proprietário para a assinatura:** Basta autenticar na sua conta do Azure.
- **Se você não for um Administrador Global e tiver permissões de proprietário na assinatura:** Antes de adicionar a assinatura ao Citrix DaaS, crie um aplicativo do Azure no seu Azure AD e adicione esse aplicativo como colaborador da assinatura. Ao adicionar essa assinatura ao Citrix DaaS, você fornece informações relevantes do aplicativo.

Adicione assinaturas do Azure gerenciadas pelo cliente se você for um Administrador Global

Essa tarefa requer permissões de Administrador Global para o diretório e permissões de proprietário para a assinatura.

1. Em **Manage > Quick Deploy**, expanda **Subscriptions** à direita.
2. Selecione **Add Azure subscription**.
3. Na página **Add Subscriptions**, selecione **Add your Azure subscription**.
4. Selecione o botão que permite que o Citrix DaaS acesse suas assinaturas do Azure em seu nome.
5. Selecione **Authenticate Azure Account**. Você será direcionado para a página de login do Azure.
6. Insira suas credenciais do Azure.
7. Você é reencaminhado automaticamente ao Citrix DaaS. A página **Add Subscription** lista as assinaturas do Azure descobertas. Use a caixa de pesquisa para filtrar a lista, se necessário. Selecione uma ou mais assinaturas. Quando terminar, selecione **Add Subscriptions**.
8. Confirme que você deseja adicionar as assinaturas selecionadas.

As assinaturas do Azure que você selecionou são listadas quando você expande a opção **Subscriptions**. As assinaturas adicionadas estão disponíveis para seleção quando você cria um catálogo ou uma imagem.

Adicione assinaturas do Azure gerenciadas pelo cliente se você não for um Administrador Global

Adicionar uma assinatura do Azure quando você não é um administrador global é um processo em duas partes:

- Antes de adicionar uma assinatura ao Citrix DaaS, crie um aplicativo no Azure AD e adicione esse aplicativo como colaborador da assinatura.
- Adicione a assinatura do Citrix DaaS, usando as informações sobre o aplicativo que você criou no Azure.

Crie um aplicativo no Azure AD e adicione-o como colaborador

1. Registre um novo aplicativo no Azure AD:
    a. Em um navegador, navegue até `<https://portal.azure.com>`.
    b. No menu superior esquerdo, selecione **Azure Active Directory**.
    c. Na lista **Manage**, selecione **App registrations**.
    d. Selecione **+ New registration**.
    e. Na página **Register an application**, forneça as seguintes informações:
        - **Name:** Insira o nome da conexão
        - **Application type:** Selecione **Web app / API**
        - **Redirect URI:** deixe em branco
    f. Selecione **Create**.
2. Crie a chave de acesso secreta do aplicativo e adicione a atribuição de função:
    a. No procedimento anterior, selecione **App Registration** para ver os detalhes.
    b. Anote o **Application ID** e o **Directory ID**. Você usará isso mais tarde ao adicionar sua assinatura ao Citrix DaaS.
    c. Em **Manage**, selecione **Certificates & secrets**.
    d. Na página **Client secrets**, selecione **+ New client secret**.
    e. Na página **Add a client secret**, forneça uma descrição e selecione um intervalo de expiração. Em seguida, selecione **Add**.
    f. Anote o valor do segredo do cliente. Você usará isso mais tarde ao adicionar sua assinatura ao Citrix DaaS.

g. Selecione a assinatura do Azure que você deseja vincular (adicionar) ao Citrix DaaS e, em seguida, selecione **Access control (IAM)**.

h. Na caixa **Add a role assignment** de função, selecione **Add**.

i. Na guia **Add role assignment**, selecione o seguinte:

- **Role:** Colaborador
- **Assign access to:** usuário, grupo ou entidade de serviço do Azure AD
- **Select:** O nome do aplicativo Azure que você criou anteriormente.

j. Selecione **Save**.

Adicione sua assinatura do Citrix DaaS

Você precisa do ID do aplicativo, do ID do diretório e do valor do segredo do cliente do aplicativo criado no Azure AD.

1. Em **Manage > Quick Deploy**, expanda **Subscriptions** à direita.
2. Selecione **Add Azure subscription**.
3. Na página **Add Subscriptions**, selecione **Add your Azure subscriptions**.
4. Selecione **I have an Azure App with contributor role to the subscription**.
5. Insira o ID do locatário (ID do diretório), o ID do cliente (ID do aplicativo) e o segredo do cliente para o aplicativo que você criou no Azure.
6. Selecione **Selecione sua assinatura** e, em seguida, selecione a assinatura desejada.

Posteriormente, na página **Details** da assinatura no painel Citrix DaaS, você pode atualizar o segredo do cliente ou substituir o aplicativo Azure no menu de reticências.

Se o Citrix DaaS não puder acessar uma assinatura do Azure depois que ela for adicionada, não serão permitidas várias ações de gerenciamento de energia de catálogo e das máquinas. Uma mensagem fornece uma opção para adicionar a assinatura novamente. Se a assinatura foi originalmente adicionada usando um aplicativo do Azure, você pode substituir o aplicativo do Azure.

Adicionar assinaturas do Citrix Managed Azure

Uma assinatura do Citrix Managed Azure oferece suporte a um determinado número de máquinas. (Nesse contexto, a expressão *máquina* se refere a VMs que têm um Citrix VDA instalado. Essas máquinas fornecem aplicativos e desktops aos usuários. A expressão não inclui outras máquinas em um local de recurso, como Cloud Connectors.)

Se sua assinatura do Citrix Managed Azure provavelmente atingirá seu limite em breve e você tiver licenças Citrix suficientes, poderá solicitar outra assinatura do Citrix Managed Azure. O painel contém uma notificação quando você está perto do limite.

Você não pode criar um catálogo (ou adicionar máquinas a um catálogo) se o número total de máquinas para todos os catálogos que usam essa assinatura do Citrix Managed Azure exceder o limite.

Por exemplo, suponha um limite hipotético de 1.000 máquinas por assinatura do Citrix Managed Azure.

- Digamos que você tenha dois catálogos (`Cat1` e `Cat2`) que usam a mesma assinatura do Citrix Managed Azure. `Cat1` atualmente contém 500 máquinas e `Cat2` tem 250.
- Ao planejar as necessidades futuras de capacidade, você adiciona 200 máquinas a `Cat2`. A assinatura do Citrix Managed Azure agora oferece suporte a 950 máquinas (500 em `Cat 1` e 450 em `Cat 2`). O painel indica que a assinatura está perto do limite.
- Quando você precisar de mais 75 máquinas, não poderá usar essa assinatura para criar um catálogo com 75 máquinas (ou adicionar 75 máquinas a um catálogo existente). Isso excederia o limite de assinatura. Em vez disso, você solicita outra assinatura do Citrix Managed Azure. Em seguida, você pode criar um catálogo usando essa assinatura.

Quando você tiver mais de uma assinatura do Citrix Managed Azure:

- Nada é compartilhado entre essas assinaturas.
- Cada assinatura tem um nome exclusivo.
- Você pode escolher entre as assinaturas do Citrix Managed Azure (e todas as assinaturas do Azure gerenciadas pelo cliente que você adicionou) quando:
  - Criação de um catálogo.
  - Construindo ou importando uma imagem.
  - Criação de um emparelhamento VNet ou conexão SD-WAN.

Requisito:

- Você deve ter licenças Citrix suficientes para garantir a adição de outra assinatura do Citrix Managed Azure. Usando o exemplo hipotético anterior, se você tiver 2.000 licenças Citrix anteriormente à implantação de pelo menos 1.500 máquinas por meio de assinaturas do Citrix Managed, poderá adicionar outra assinatura do Citrix Managed Azure.

Para adicionar uma assinatura do Citrix Managed Azure:

1. Entre em contato com seu representante Citrix para solicitar outra assinatura do Citrix Managed Azure. Você será notificado quando puder continuar.
2. Em **Manage > Quick Deploy**, expanda **Subscriptions** à direita.
3. Selecione **Add Azure subscription**.
4. Na página **Add Subscriptions**, selecione **Add a Citrix Managed Azure subscription**.
5. Na página **Add a Citrix Managed Subscription**, selecione **Add Subscription** na parte inferior da página.

Se você for notificado de que ocorreu um erro durante a criação de uma assinatura do Citrix Managed Azure, entre em contato com o Suporte Citrix.

Remover assinaturas do Azure

Antes de remover uma assinatura do Azure, você deve excluir todos os catálogos e imagens que a usam.

Se você tiver uma ou mais assinaturas do Citrix Managed Azure, não poderá remover todas elas. Pelo menos uma deve permanecer.

1. Em **Manage > Quick Deploy**, expanda **Subscriptions** à direita.
2. Selecione a entrada da assinatura.
3. Na guia **Details**, selecione **Remove Subscription**.
4. Selecione **Authenticate Azure Account**. Você será direcionado para a página de login do Azure.
5. Insira suas credenciais do Azure.
6. Você é reencaminhado automaticamente ao Citrix DaaS. Confirme a exclusão e selecione **Yes, Delete Subscription**.

Atualizar segredos de clientes expirados

Quando o segredo de cliente de uma assinatura expira, você não pode criar catálogos de máquinas para ele, e um alerta aparece na entrada da assinatura. Para resolver esse problema, você tem duas opções:

- Atualizar o segredo de cliente do aplicativo do Azure em uso
- Mudar para um aplicativo do Azure com uma data de expiração válida

Atualizar o segredo de cliente do aplicativo do Azure em uso

Para continuar usando o aplicativo do Azure existente para acessar os recursos do Azure, siga estas etapas:

1. No Azure, crie um segredo de cliente para o aplicativo do Azure em uso. Anote o novo segredo e a data de validade para uso futuro. Para obter mais informações, consulte Criar um segredo de aplicativo no Azure.
2. No DaaS, forneça as informações do segredo recém-criado para a assinatura. As etapas detalhadas são as seguintes:
    a. No painel **Manage > Azure Quick Deploy** no Citrix DaaS for Azure, expanda **Cloud Subscriptions** à direita.
    b. Clique na assinatura que precisa ter o segredo atualizado.
    c. Na página de assinatura exibida, clique no menu de reticências no painel **Azure App Details** e selecione **Update Client Secret**.
    d. Na página **Update Client Secret**, digite os novos dados em **Client Secret** e **Secret Expiration Date**.
    e. Clique em **Update Secret**.

Mudar para um aplicativo do Azure com uma data de expiração válida

Para mudar para um aplicativo do Azure válido para acessar os recursos do Azure, obtenha as informações necessárias do aplicativo e forneça-as à assinatura seguindo estas etapas:

1. No Azure, obtenha um aplicativo do Azure válido e anote seus detalhes. Certifique-se de que o novo aplicativo do Azure tenha a função *Contributor* atribuída. Para obter mais informações, consulte Crie um aplicativo no Azure AD e adicione-o como colaborador.
2. No DaaS, forneça detalhes do aplicativo do Azure para a assinatura. As etapas detalhadas são as seguintes:
    a. No painel **Manage > Azure Quick Deploy** no Citrix DaaS for Azure, expanda **Cloud Subscriptions** à direita.
    b. Clique na assinatura que precisa ter o segredo atualizado.
    c. Na página de assinatura exibida, clique no menu de reticências no painel **Azure App Details** e selecione **Replace Azure App.**

d. Na página **Replace Azure App**, digite os detalhes do novo aplicativo do Azure nos campos correspondentes a **Directory (tenant) ID**, **Application (client) ID**, **Client Secret** e **Secret Expiration Date for the service principal**.

e. Clique em **Replace App**.

Criar catálogos usando o Quick Deploy

Use os procedimentos neste artigo para criar um catálogo de máquinas do Microsoft Azure por meio da interface de gerenciamento do Quick Deploy.

Analise todo o procedimento antes de criar um catálogo, para saber o que esperar.

Para criar um catálogo usando a interface Full Configuration, consulte Criar catálogos de máquinas.

Tipos de máquina

Um catálogo de Quick Deploy pode conter um dos seguintes tipos de máquinas:

- **Static:** o catálogo contém máquinas estáticas de sessão única (também conhecidas como desktops pessoais, dedicados ou persistentes). Static significa que, quando um usuário inicia uma área de trabalho, essa área de trabalho “pertence” a esse usuário. Todas as alterações feitas pelo usuário na área de trabalho são mantidas no logoff. Mais tarde, quando esse usuário retornar ao Citrix Workspace e iniciar uma área de trabalho, ela será a mesma área de trabalho.
- **Random:** o catálogo contém máquinas aleatórias de sessão única (também conhecidas como desktops não persistentes). Aleatório significa que quando um usuário inicia uma área de trabalho, todas as alterações feitas por ele nessa área de trabalho são descartadas após o logoff. Mais tarde, quando esse usuário retornar ao Citrix Workspace e iniciar uma área de trabalho, ela pode ou não ser a mesma área de trabalho.
- **Multi-session:** o catálogo contém máquinas com aplicativos e desktops. Mais de um usuário pode acessar cada uma dessas máquinas simultaneamente. Os usuários podem iniciar uma área de trabalho ou aplicativos em seu espaço de trabalho. As sessões do aplicativo podem ser compartilhadas. O compartilhamento de sessão não é permitido entre um aplicativo e um desktop.

    - Ao criar um catálogo de várias sessões, você seleciona a carga de trabalho: leve (como entrada de dados), média (como aplicativos de escritório), pesada (como engenharia) ou

personalizada. Cada opção representa um número específico de máquinas e sessões por máquina, o que gera o número total de sessões que o catálogo suporta.

- Se você selecionar a carga de trabalho personalizada, selecione entre as combinações disponíveis de CPUs, RAM e armazenamento. Digite o número de máquinas e sessões por máquina, o que gera o número total de sessões que o catálogo suporta.

Ao implantar desktops, os tipos de máquina estáticos e aleatórios às vezes são chamados de “tipos de desktop”.

Maneiras de criar um catálogo usando o Quick Deploy

Há várias maneiras de criar e configurar um catálogo:

- A **criação rápida** é a maneira mais rápida de começar. Você fornece informações mínimas, e o Citrix DaaS (antigo serviço Citrix Virtual Apps and Desktops) cuida do resto. Um catálogo de criação rápida é ótimo para um ambiente de teste ou prova de conceito.
- A **criação personalizada** permite mais opções de configuração do que a criação rápida. É mais adequada para um ambiente de produção do que um catálogo de criação rápida.
- Os catálogos **Remote PC Access** contêm máquinas existentes (geralmente físicas) que os usuários acessam remotamente. Para obter detalhes e instruções sobre esses catálogos, consulte Acesso ao PC remoto.

Aqui está uma comparação entre criação rápida e criação personalizada:

CRIAÇÃO RÁPIDA	CRIAÇÃO PERSONALIZADA
Menos informações para fornecer.	Mais informações para fornecer.
Menos opções para alguns recursos.	Mais opções para alguns recursos.
Autenticação de usuário do Azure Active Directory gerenciada pela Citrix.	Opções: Azure Active Directory gerenciado pela Citrix ou seu Active Directory/Azure Active Directory.
Sem conexão com sua rede local.	Opções: Sem conexão com sua rede local, emparelhamento de VNet do Azure e SD-WAN.
Usa uma imagem do Windows 10 preparada pela Citrix. Essa imagem contém um VDA de desktop atual.	Opções: imagens preparadas pela Citrix, suas imagens que você importa do Azure ou imagens que você criou no Citrix DaaS a partir

CRIAÇÃO RÁPIDA	CRIAÇÃO PERSONALIZADA
	de uma imagem preparada ou importada pela Citrix.
Cada desktop tem armazenamento em disco padrão (HDD) do Azure.	Várias opções de armazenamento estão disponíveis.
Somente desktops estáticos.	Desktops estáticos, aleatórios ou com várias sessões.
Um cronograma de gerenciamento de energia não pode ser configurado durante a criação. A máquina que hospeda a área de trabalho é desligada quando a sessão termina. (Você pode alterar essa configuração mais tarde.)	Um cronograma de gerenciamento de energia pode ser configurado durante a criação. (Uma programação de gerenciamento de energia do Quick Deploy difere de uma programação de gerenciamento de energia que você pode criar usando a interface de gerenciamento Full Configuration.)
É necessário usar uma assinatura do Citrix Managed Azure.	Pode usar a assinatura do Citrix Managed Azure ou sua própria assinatura do Azure.

Para obter detalhes sobre o procedimento, consulte:

- Crie um catálogo do Quick Deploy usando a criação rápida
- Criar um catálogo do Quick Deploy usando a criação personalizada

> **Importante:**
>
> Quando você cria um catálogo (ou uma imagem) usando uma assinatura do Citrix Managed Azure pela primeira vez, você é solicitado a reconhecer e consentir com sua responsabilidade pelos valores cobrados. Os lembretes desse consentimento também podem aparecer ao criar mais catálogos ou imagens usando a assinatura do Citrix Managed Azure.

Crie um catálogo do Quick Deploy usando a criação rápida

O método de criação rápida usa uma assinatura do Citrix Managed Azure e uma imagem do Windows 10 preparada pela Citrix para criar um catálogo contendo máquinas estáticas. As configurações de gerenciamento de energia usam os valores predefinidos de Cost Saver. Não há

conexão com sua rede corporativa. Os usuários devem ser adicionados usando o Citrix Managed Azure AD.

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **My Services > DaaS**.
3. Selecione **Manage > Quick Deploy**.
4. Se ainda não tiver sido criado nenhum catálogo, você será direcionado para a página de **boas-vindas**. Escolha uma das seguintes opções:
   - Configure o catálogo nesta página. Continue com as etapas de 6 a 10.

     
   - Selecione **Get Started**. Você será direcionado para o painel **Manage > Quick Deploy**. Selecione **Create Catalog**.
5. Se um catálogo já tiver sido criado (e você estiver criando outro), você será direcionado para o painel **Manage > Quick Deploy**. Selecione **Create Catalog**.

   
6. Selecione **Quick Create** na parte superior da página, se ainda não estiver selecionada.

   
   - **Machine performance:** Selecione o tipo de máquina. Cada opção tem uma combinação exclusiva de CPUs, RAM e armazenamento. Máquinas de alto desempenho têm custos mensais mais altos.
   - **Region:** Selecione uma região onde você deseja que as máquinas sejam criadas. Você pode selecionar uma região próxima aos seus usuários.
   - **Name:** digite um nome para o catálogo. Esse campo é obrigatório e não há valor padrão.
   - **Number of machines:** digite o número de máquinas que você deseja.
7. Quando terminar, selecione **Create Catalog**. (Se você estiver criando o primeiro catálogo na página **Welcome**, selecione **Quick Create Desktops**.)
8. Se este for o primeiro catálogo que você está criando por meio de uma assinatura do Citrix Managed Azure, quando solicitado, assuma a responsabilidade pelas cobranças correlatas.

Enquanto o catálogo está sendo criado, o nome do catálogo é adicionado à lista de catálogos, indicando seu progresso na criação.

O Citrix DaaS também cria automaticamente um local de recursos e adiciona dois conectores do Citrix Cloud.

O que fazer a seguir:

- Você pode adicionar usuários ao diretório Managed Azure AD enquanto o catálogo está sendo criado.
- Depois que o catálogo for criado, adicione usuários ao catálogo.

Criar um catálogo do Quick Deploy usando a criação personalizada

Se você estiver usando uma assinatura do Citrix Managed Azure e planeja usar uma conexão com seus recursos de rede local, crie essa conexão de rede antes de criar o catálogo. Para permitir que seus usuários acessem seus recursos locais ou outros recursos de rede, você também precisa de informações do Active Directory para esse local.

Se você não tiver uma assinatura do Citrix Managed Azure, será possível:

- Solicite o Azure Consumption Fund no Azure Marketplace, que fornece uma assinatura do Citrix Managed Azure.
- Importe (adicione) uma ou mais de suas próprias assinaturas do Azure para o Citrix DaaS antes de criar um catálogo.

Para criar um catálogo:

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **My Services > DaaS**.
3. Selecione **Manage > Quick Deploy**.
4. Se ainda não tiver sido criado nenhum catálogo, você será direcionado para a página de **boas-vindas**. Selecione **Get Started**. No final da página de introdução, você será direcionado para o painel **Manage > Quick Deploy**. Selecione **Create Catalog**.

   Se já tiver sido criado um catálogo, você será direcionado para o painel **Manage > Quick Deploy**. Selecione **Create Catalog**.

5. Selecione **Custom Create** na parte superior da página, se ainda não estiver selecionado.

6. Preencha os campos a seguir. (Alguns campos são válidos somente para determinados tipos de máquinas. A ordem dos campos pode ser diferente.)

   - **Machine type**. Selecione um tipo de máquina. Para obter detalhes, consulte Tipos de máquina.
   - **Subscription**. Selecione uma assinatura do Azure.
   - **Master image:** selecione uma imagem do sistema operacional a ser usada para as máquinas do catálogo.
   - **Network connection:** selecione a conexão de rede a ser usada para acessar recursos em sua rede.

     Se você selecionou uma assinatura do Citrix Managed Azure, as opções são:

     - **No Connectivity:** os usuários não podem acessar locais e recursos em sua rede corporativa local.
     - *Connections:* selecione uma conexão criada anteriormente, como um emparelhamento de VNet ou conexão SD-WAN.

     Se você selecionou uma assinatura do Azure gerenciada pelo cliente, selecione o grupo de recursos, a rede virtual e a sub-rede apropriados.
   - **Region:** (Disponível somente se você tiver selecionado **No Connectivity** em **Network connection**.) Selecione uma região onde você deseja que as áreas de trabalho sejam criadas. Você pode selecionar uma região próxima aos seus usuários.

     Se você tiver selecionado uma conexão em **Network connection**, o catálogo usa a região dessa rede.
   - **Qualify for Linux compute rates?** (Disponível somente se você tiver selecionado uma imagem do Windows.) Você pode economizar dinheiro ao usar sua licença qualificada ou o Azure Hybrid Benefit.

     Windows Virtual Desktop benefit: licenças qualificadas do Windows 10 ou Windows 7 por usuário para:

     - Microsoft 365 E3/ES
     - Benefícios de uso do Microsoft 365 A3/AS/Student
     - Microsoft 365 F3
     - Microsoft 365 Business Premium
     - Windows 10 Enterprise E3/E5

  - Windows 10 Education A3/A5
  - Windows 10 VDA por usuário

  Licença por usuário ou por dispositivo da RDS CAL com Software Assurance para cargas de trabalho do Windows Server.

  Azure Hybrid benefit: licenças do Windows Server com o Software Assurance ativo ou as licenças de assinatura qualificadas equivalentes. Veja `<https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>`.

- **Machine:**
  - **Storage type**. HDD ou SSD.
  - **Machine performance** (para o tipo de máquina **Static** ou **Random**) ou **Workload** (para o tipo de máquina de várias sessões). As opções incluem somente opções que correspondem ao tipo de geração (gen1 ou gen2) da imagem selecionada.

    Se você selecionar a carga de trabalho personalizada, digite o número de máquinas e sessões por máquina no campo **Machine Performance**.
  - **Machines**. Quantas máquinas você quer neste catálogo.
- **Machine naming scheme:** consulte Esquema de nomenclatura de máquinas.
- **Name:** digite um nome para o catálogo. Esse nome aparece no painel **Manage**.
- **Programação de energia:** Por padrão, a caixa de seleção **I'll configure this later** está marcada. Para obter detalhes, consulte Gerenciar programações de gerenciamento de energia. (Esse cronograma de gerenciamento de energia difere dos recursos de gerenciamento de energia disponíveis na interface de gerenciamento Full Configuration do Citrix DaaS.)
- **Join the local Active Directory domain:** (Disponível somente se você tiver selecionado uma conexão de emparelhamento VNet do Azure em **Network connection**.) Selecione **Yes** ou **No**. Se você selecionar **Yes**, digite:
  - FQDN do domínio (por exemplo, Contoso.com).
  - Organization Unit: Para usar a UO (Computadores) padrão, deixe este campo vazio.
  - Citrix Daas account name: deve ser um administrador de domínio ou empresa no formato nome@domínio ou domínio\nome.
  - Senha para o nome da conta Citrix DaaS.

- **Advanced settings:** consulte Configurações de localização de recursos ao criar um catálogo.

7. Quando terminar, selecione **Create Catalog**.
8. Se este for o primeiro catálogo que você está criando por meio de uma assinatura do Citrix Managed Azure, quando solicitado, assuma a responsabilidade pelas cobranças correlatas.

O painel **Manage > Quick Deploy** indica quando seu catálogo é criado. O Citrix DaaS também cria automaticamente um local de recursos e adiciona dois conectores do Citrix Cloud.

O que fazer a seguir:

- Se você ainda não fez isso, configure o método de autenticação para que seus usuários se autentiquem no Citrix Workspace.
- Depois que o catálogo for criado, adicione usuários ao catálogo.
- Se você criou um catálogo de várias sessões, adicione aplicativos (antes ou depois de adicionar usuários).

Configurações de localização de recursos ao criar um catálogo

Ao criar um catálogo, você pode, opcionalmente, definir várias configurações de localização de recursos.

Quando você seleciona **Advanced settings** na caixa de diálogo de criação de catálogo, o Citrix DaaS recupera as informações de localização do recurso.

- Se você já tiver um local de recurso para o domínio e a conexão de rede selecionados para o catálogo, poderá salvá-lo para uso pelo catálogo que está criando.

  Se esse local de recurso tiver apenas um Cloud Connector, outro será instalado automaticamente. Opcionalmente, você pode especificar configurações avançadas para o Cloud Connector que está adicionando.
- Se você não tiver um local de recurso configurado para o domínio e a conexão de rede selecionados para o catálogo, será solicitado que você configure um.

Defina as configurações avançadas:

- (Obrigatório somente quando o local do recurso já está configurado.) Um nome para o local do recurso.
- Tipo de conectividade externa: por meio do serviço Citrix Gateway ou de dentro de sua rede corporativa.

- Configurações do Cloud Connector:
  - (Disponível somente ao usar uma assinatura do Azure gerenciada pelo cliente) Machine performance. Essa seleção é usada para os Cloud Connectors no local do recurso.
  - (Disponível somente ao usar uma assinatura do Azure gerenciada pelo cliente) Azure resource group. Essa seleção é usada para os Cloud Connectors no local do recurso. O padrão é o último grupo de recursos usado pelo local do recurso (se aplicável).
  - Organizational Unit (OU). O padrão é a UO usada pela última vez pelo local do recurso (se aplicável).

Quando terminar as configurações avançadas, selecione **Save** para retornar à caixa de diálogo de criação do catálogo.

Depois de criar um catálogo, várias ações de localização de recursos estarão disponíveis. Para obter detalhes, consulte Resource location actions.

Esquema de nomenclatura de máquinas

Para especificar um esquema de nomenclatura de máquinas ao criar um catálogo, selecione **Specify machine naming scheme**. Use de 1 a 4 caracteres curinga (marcas de hash) para indicar onde números ou letras sequenciais aparecem no nome. Regras:

- O esquema de nomenclatura deve conter pelo menos um curinga, mas não mais do que quatro curingas. Todos os curingas devem estar juntos.
- O nome inteiro, incluindo curingas, deve ter entre 2 e 15 caracteres.
- Um nome não pode incluir espaços em branco (espaços), barras, barras invertidas, dois-pontos, asteriscos, colchetes angulares, barras verticais, vírgulas, sinais de til, pontos de exclamação, símbolos de arroba, cifrões, sinais de porcentagem, sinais de circunflexo, parênteses, chaves ou sublinhados.
- Um nome não pode começar com um ponto final.
- Um nome não pode conter somente números.
- Não use as seguintes letras no final de um nome: `-GATEWAY`, `-GW` e `-TAC`.

Indique se os valores sequenciais são números (0-9) ou letras (A-Z):

Por exemplo, um esquema de nomenclatura de `PC-Sales-##` (com **0-9** selecionado) resulta em contas de computador nomeadas `PC-Sales-01`, `PC-Sales-02`, `PC-Sales-03` e assim por diante.

Deixe espaço suficiente para a expansão.

- Por exemplo, um esquema de nomeação com 2 curingas e 13 outros caracteres (por exemplo, `MachineSales-##`) usa o número máximo de caracteres (15).
- Quando o catálogo contiver 99 máquinas, a próxima criação da máquina será malsucedida. O Citrix DaaS tenta criar uma máquina com três dígitos (100), mas isso criaria um nome com 16 caracteres. O máximo é 15.
- Então, neste exemplo, um nome mais curto (por exemplo, `PC-Sales-##`) permite escalar para além de 99 máquinas.

Se você não especificar um esquema de nomenclatura de máquinas, o Citrix DaaS usará o esquema de nomenclatura padrão `DAS%%%%%-**-###`.

- `%%%%%` = cinco caracteres alfanuméricos aleatórios que correspondem ao prefixo de localização do recurso
- `**` = dois caracteres alfanuméricos aleatórios para o catálogo
- `###` = três dígitos.

Informações correlatas

- Catálogos de acesso remoto ao PC
- Criar um catálogo em uma rede que usa um servidor proxy
- Exibir informações do catálogo
- Gerenciar catálogos no Quick Deploy

Gerenciar catálogos no Quick Deploy

Este artigo descreve as tarefas de gerenciamento de catálogo que você pode usar para gerenciar catálogos que foram criados no Quick Deploy.

Lembre-se: se você tiver usado o Quick Deploy para criar um catálogo e, em seguida, usar a interface Full Configuration para executar tarefas de gerenciamento nesse catálogo, não será mais possível usar a interface Quick Deploy para esse catálogo.

(Para obter informações sobre o gerenciamento de catálogos na interface de gerenciamento de Full Configuration, consulte Manage machine catalogs.)

Adicionar máquinas a um catálogo

Enquanto as máquinas estão sendo adicionadas a um catálogo de Quick Deploy, você não pode fazer nenhuma outra alteração nesse catálogo.

1. Em **Manage > Quick Deploy**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Machines**, selecione **Add Machines to Catalog**.



3. Insira o número de máquinas que você deseja adicionar ao catálogo.



4. (Válido somente se o catálogo tiver ingressado no domínio.) Digite o nome de usuário e a senha da conta Citrix DaaS (antigo serviço Citrix Virtual Apps and Desktops).
5. Selecione **Add Machines to Catalog**.

Você não pode reduzir a contagem de máquinas para um catálogo. No entanto, você pode usar as configurações de programação de gerenciamento de energia para controlar quantas máquinas estão ligadas ou excluir máquinas da guia **Machines**. Consulte Manage machines in a catalog para obter informações sobre como excluir máquinas na guia **Machines**.

Alterar o número de sessões por máquina

Alterar o número de sessões por máquina com várias sessões pode ter influência na experiência dos usuários. Aumentar esse valor pode reduzir os recursos computacionais alocados para sessões simultâneas.

Recomendação: observe seus dados de uso para determinar o equilíbrio adequado entre a experiência do usuário e o custo.

1. Em **Manage > Quick Deploy**, selecione um catálogo que contenha máquinas com várias sessões.
2. Na guia **Details**, selecione **Edit** ao lado de **Sessions per Machine**.
3. Insira um novo número de sessões por máquina.
4. Selecione **Update Number of Sessions**.
5. Confirme sua solicitação.

Essa alteração não afeta as sessões atuais. Quando você altera o número máximo de sessões para um valor menor que o das sessões ativas atualmente de uma máquina, o novo valor é implementado por meio do atrito normal das sessões ativas.

Se ocorrer uma falha antes do início do processo de atualização, a exibição **Details** do catálogo manterá o número correto de sessões. Se ocorrer uma falha durante o processo de atualização, a exibição indicará o número de sessões desejadas.

Gerenciar máquinas em um catálogo

> **Nota:**
>
> Muitas das ações que estão disponíveis em **Manage > Quick Deploy** também estão disponíveis na guia **Monitor** em Quick Deploy.

Para selecionar ações em **Manage > Quick Deploy**:

1. Em **Manage > Quick Deploy**, clique em qualquer lugar na entrada de um catálogo.
2. Na guia **Machines**, localize a máquina que você deseja gerenciar. No menu de reticências dessa máquina, selecione a ação desejada:

   - **Restart:** reinicia a máquina selecionada.
   - **Start:** inicia a máquina selecionada. Essa ação estará disponível somente se a máquina estiver desligada.
   - **Shutdown:** desliga a máquina selecionada. Essa ação estará disponível somente se a máquina estiver ligada.
   - **Turn maintenance mode on/off:** ativa o modo de manutenção (se estiver desligado) ou desligado (se estiver ligado) para a máquina selecionada. Por padrão, o modo de manutenção está desativado para uma máquina.

     Ativar o modo de manutenção impede que sejam estabelecidas novas conexões a essa máquina. Os usuários podem se conectar a sessões existentes nessa máquina, mas não podem iniciar novas sessões nessa máquina.

     Você pode colocar uma máquina no modo de manutenção antes de aplicar patches ou para solucionar problemas.
   - **Delete:** exclui a máquina selecionada. Essa ação está disponível somente quando a contagem de sessões da máquina é zero. Confirme a exclusão.

     Quando uma máquina é excluída, todos os dados nela contidos são removidos.

- **Force restart:** força a reinicialização da máquina selecionada. Selecione essa ação somente se uma ação **Restart** não surtir efeito na máquina.

Adicionar aplicativos a um catálogo

1. Em **Manage > Quick Deploy**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Desktop and Apps**, selecione **Manage Apps**.



3. Selecione como você está adicionando aplicativos: no menu **Start** das máquinas no catálogo ou em um caminho diferente nas máquinas.
4. Para adicionar aplicativos do menu **Start** :



   - Selecione os aplicativos disponíveis na coluna da esquerda. (Use a opção **Search** para personalizar a lista de aplicativos.) Selecione a seta para a direita entre as colunas. Os aplicativos selecionados são movidos para a coluna da direita.
   - Da mesma forma, para remover aplicativos, selecione-os na coluna da direita. Selecione a seta para a esquerda entre as colunas.
   - Se o menu **Start** tiver mais de uma versão do mesmo aplicativo, com o mesmo nome, você poderá adicionar apenas uma. Para adicionar outra versão desse aplicativo, edite essa versão para alterar seu nome. Em seguida, você pode adicionar essa versão do aplicativo.
5. Para adicionar aplicativos por caminho:



   - Insira o nome do aplicativo. Esse é o nome que os usuários veem no Citrix Workspace.
   - O ícone mostrado é o ícone que os usuários veem no Citrix Workspace. Para selecionar outro ícone, selecione **Change icon** e navegue até o ícone que deseja exibir.
   - (Opcional) Insira uma descrição do aplicativo.
   - Insira o caminho para o aplicativo. Esse campo é obrigatório. Opcionalmente, adicione parâmetros de linha de comando e o diretório de trabalho. Para obter detalhes sobre os parâmetros da linha de comando, consulte Passar parâmetros para aplicativos publicados.
6. Quando terminar, selecione **Close**.

Nos VDAs do Windows Server 2019, alguns ícones de aplicativos podem não aparecer corretamente durante a configuração e no espaço de trabalho dos usuários. Como solução

alternativa, depois que o aplicativo for publicado, edite o aplicativo e use o recurso **Change icon** para atribuir um ícone diferente que seja exibido corretamente.

Editar um aplicativo em um catálogo

1. Em **Manage > Quick Deploy**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Desktop and Apps**, clique em qualquer lugar na linha que contém o aplicativo que você deseja editar.
3. Selecione o ícone de lápis.

4. Digite as alterações em qualquer um dos seguintes campos:

   - **Name:** o nome que os usuários veem no Citrix Workspace.
   - **Descrição**
   - **Path:** o caminho para o executável.
   - **Command line parameters:** para obter detalhes, consulte Passar parâmetros para aplicativos publicados.
   - **Working directory**

5. Para alterar o ícone que os usuários veem no Citrix Workspace, selecione **Change icon** e navegue até o ícone que deseja exibir.
6. Quando terminar, selecione **Save**.

Passar parâmetros para aplicativos publicados

Quando você associa um aplicativo publicado a tipos de arquivo, os símbolos de percentual e estrela (entre aspas duplas) são acrescidos ao final da linha de comando. Esses símbolos atuam como um espaço reservado para parâmetros passados para dispositivos do usuário.

- Se um aplicativo publicado não for iniciado quando esperado, verifique se sua linha de comando contém os símbolos corretos. Por padrão, os parâmetros fornecidos pelos dispositivos do usuário são validados quando os símbolos são acrescentados.

  Para aplicativos publicados que usam parâmetros personalizados fornecidos pelo dispositivo do usuário, os símbolos são acrescentados à linha de comando para deixar de lado a validação da linha de comando. Se você não vir esses símbolos em uma linha de comando para o aplicativo, adicione-os manualmente.

- Se o caminho para o arquivo executável incluir nomes de diretório com espaços (como `“C:\Program Files”`), inclua a linha de comando do aplicativo entre aspas duplas para indicar que o espaço pertence à linha de comando. Adicione aspas duplas ao redor do caminho e outro conjunto de aspas duplas ao redor dos símbolos de porcentagem e asterisco. Adicione um espaço entre as aspas de fechamento para o caminho e as aspas de abertura para os símbolos de porcentagem e asterisco.

  Por exemplo, a linha de comando para o aplicativo publicado Windows Media Player é: `“C:\Program Files\Windows Media Player\mplayer1.exe” “%*”`

Remover aplicativos de um catálogo

Remover um aplicativo de um catálogo não o remove das máquinas. Isso apenas impede que ele apareça no Citrix Workspace.

1. Em **Manage > Quick Deploy**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Desktop and Apps**, selecione o ícone de lixeira ao lado dos aplicativos que você deseja remover.

Excluir um catálogo

Quando você exclui um catálogo, todas as máquinas no catálogo são destruídas permanentemente. A exclusão de um catálogo não pode ser revertida.

1. Em **Manage > Quick Deploy**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Detalhes**, selecione **Excluir catálogo**.
3. Confirme a exclusão.

Para ajudar a identificar contas residuais de máquinas do Active Directory que você deve excluir, faça o download de uma lista de nomes de máquina e do Cloud Connector.

Gerenciar programações de gerenciamento de energia

Um cronograma de gerenciamento de energia afeta todas as máquinas em um catálogo. Uma programação fornece:

- Experiência ideal para o usuário: as máquinas estão disponíveis para os usuários quando são necessárias.
- Segurança: as sessões da área de trabalho que permanecem ociosas por um intervalo especificado são desconectadas, exigindo que os usuários iniciem uma nova sessão em seu espaço de trabalho.

- Gerenciamento de custos e economia de energia: as máquinas com desktops que permanecem ociosas são desligadas. As máquinas são ligadas para atender à demanda programada e real.

Você pode configurar uma programação de energia ao criar um catálogo personalizado ou fazer isso mais tarde. Se nenhum agendamento for selecionado ou configurado, uma máquina será desligada quando uma sessão terminar.

Você não pode selecionar ou configurar uma programação de energia ao criar um catálogo com criação rápida. Por padrão, os catálogos de criação rápida usam a programação predefinida de Cost Saver. Você pode selecionar ou configurar uma programação diferente posteriormente para esse catálogo.

O gerenciamento de agendamento inclui:

- Saber quais informações um cronograma contém
- Criação de um cronograma

Informações em uma programação

O diagrama a seguir mostra as configurações de agendamento para um catálogo que contém máquinas com várias sessões. As configurações de um catálogo contendo máquinas de sessão única (aleatórias ou estáticas) diferem ligeiramente.



Um cronograma de gerenciamento de energia contém as seguintes informações.

Programações predefinidas

O Citrix DaaS oferece várias programações predefinidas. Você também pode configurar e salvar agendas personalizadas. Embora você possa excluir predefinições personalizadas, não é possível excluir predefinições fornecidas pela Citrix.

Time zone

Usada com a configuração de máquinas de ligar para estabelecer horas de trabalho e horas extras, com base no fuso horário selecionado.

Essa configuração é válida para todos os tipos de máquinas.

Ligar as máquinas: horas de trabalho e após o expediente

Os dias da semana e as horas de início e parada do dia que formam suas horas de trabalho. Isso geralmente indica os intervalos em que você deseja que as máquinas estejam ligadas. Qualquer

horário fora desses intervalos é considerado após o expediente. Várias configurações de agendamento permitem que você insira valores separados para horas de trabalho e horas extras. Outras configurações se aplicam o tempo todo.

Essa configuração é válida para todos os tipos de máquinas.

Disconnect desktop sessions when idle

Por quanto tempo uma área de trabalho pode permanecer ociosa (não usada) antes que a sessão seja desconectada. Depois que uma sessão é desconectada, o usuário deve ir para o Workspace e iniciar uma área de trabalho novamente. Essa é uma configuração de segurança.

Essa configuração é válida para todos os tipos de máquinas. Uma configuração se aplica o tempo todo.

Power off idle desktops

Por quanto tempo uma máquina pode permanecer desconectada antes de ser desligada. Depois que uma máquina é desligada, o usuário deve ir para o Workspace e iniciar uma área de trabalho novamente. Essa é uma configuração de economia de energia.

Por exemplo, digamos que você queira que os desktops se desconectem depois de ficarem ociosos por 10 minutos. Depois, desligar as máquinas se elas permanecerem desconectadas por mais 15 minutos.

Se um determinado usuário parar de usar a área de trabalho e sair para uma reunião de uma hora, a área de trabalho será desconectada após 10 minutos. Depois de mais 15 minutos, a máquina será desligada (25 minutos no total).

Do ponto de vista do usuário, as duas configurações de inatividade (desconexão e desligamento) têm o mesmo efeito. Se esse usuário ficar longe de sua área de trabalho por 12 minutos ou uma hora, ele deve iniciar uma área de trabalho novamente a partir do Workspace. A diferença nos dois temporizadores afeta o estado da máquina virtual que fornece a área de trabalho.

Essa configuração é válida para máquinas de sessão única (estáticas ou aleatórias). Você pode inserir valores para horas de trabalho e após o expediente.

Log off disconnected sessions

Por quanto tempo uma máquina pode permanecer desconectada antes que a sessão seja fechada.

Essa configuração é válida para máquinas com várias sessões. Uma configuração se aplica o tempo todo.

Power Off Delay

A quantidade mínima de tempo que uma máquina deve ser ligada antes de ser qualificável para desligamento (junto com outros critérios). Esta configuração evita que as máquinas “liguem e desliguem” durante as demandas oscilantes das sessões mais voláteis.

Essa configuração é válida para máquinas com várias sessões e se aplica o tempo todo.

Minimum running machines

Quantas máquinas devem permanecer ligadas, independentemente de quanto tempo estão ociosas ou desconectadas.

Essa configuração é válida para máquinas aleatórias e com várias sessões. Você pode inserir valores para horas de trabalho e após o expediente.

Capacity buffer

Um buffer de capacidade ajuda a acomodar picos repentinos na demanda, mantendo um buffer de máquinas ligado. O buffer é especificado como uma porcentagem da demanda da sessão atual. Por exemplo, se houver 100 sessões ativas e o buffer de capacidade for 10%, o Citrix DaaS fornecerá capacidade para 110 sessões. Um aumento na demanda pode ocorrer durante o horário de trabalho ou a adição de novas máquinas ao catálogo.

Um valor menor diminui o custo. Um valor mais alto ajuda a garantir uma experiência de usuário otimizada. Ao iniciar sessões, os usuários não precisam esperar que máquinas extras sejam ligadas.

Quando há máquinas mais do que suficientes para suportar o número de máquinas ligadas necessárias no catálogo (incluindo o buffer de capacidade), as máquinas extras são desligadas. O desligamento pode ocorrer devido a horários fora de pico, logoffs de sessão ou menos máquinas no catálogo. A decisão de desligar uma máquina deve atender aos seguintes critérios:

- A máquina está ligada e não está no modo de manutenção.
- A máquina está registrada como disponível ou aguardando registro após ser ligada.
- A máquina não tem sessões ativas. Todas as sessões restantes foram encerradas. (A máquina ficou ociosa durante o período de tempo limite de inatividade.)
- A máquina foi ligada por pelo menos “X” minutos, onde “X” é o atraso de desligamento especificado para o catálogo.

  Em um catálogo estático, depois que todas as máquinas no catálogo são atribuídas, o buffer de capacidade não desempenha um papel na ativação ou desativação das máquinas.

Essa configuração é válida para todos os tipos de máquinas. Você pode inserir valores para horas de trabalho e após o expediente.

Crie um cronograma de gerenciamento de energia

1. Em **Manage > Quick Deploy**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Power Management**, determine se alguma das programações predefinidas (no menu na parte superior) atende às suas necessidades. Selecione uma predefinição para ver os valores que ela usa. Se quiser usar uma predefinição, deixe-a selecionada.
3. Se você alterar os valores em qualquer campo (como dias, horas ou intervalos), a seleção predefinida será alterada para **Custom** automaticamente. Um asterisco indica que as configurações personalizadas não foram salvas.
4. Defina os valores desejados para a programação personalizada.
5. Selecione **Custom** na parte superior e salve as configurações atuais como uma nova predefinição. Insira um nome para a nova predefinição e selecione a marca de seleção.
6. Quando terminar, selecione **Save Changes**.

Posteriormente, você pode editar ou excluir uma predefinição personalizada usando os ícones de lápis ou lixeira no menu **Presets**. Não é possível editar ou excluir predefinições comuns.

Informações correlatas

- Atualizar um catálogo com uma nova imagem
- Adicionar e remover usuários em um catálogo

Introdução ao Quick Deploy

Este artigo resume as tarefas de configuração para fornecer desktops e aplicativos usando a interface Quick Deploy do Citrix DaaS (antigo serviço Citrix Virtual Apps and Desktops). Recomendamos que você revise cada procedimento antes de realizá-lo na prática para que você saiba o que esperar.

Para usar o Quick Deploy para configurar uma implantação de acesso remoto ao PC, consulte Remote PC Access.

Resumo da tarefa de configuração

As seções a seguir deste artigo orientam você nas tarefas de configuração:

1. Revise e conclua as tarefas necessárias nos requisitos e na preparação do sistema.

2. Configure uma implantação rápida de prova de conceito ou uma implantação de produção.
3. Forneça a URL do espaço de trabalho para seus usuários.

Requisitos e preparação do sistema

- Inscreva-se no Citrix Cloud e no Citrix DaaS.

  Além disso, se você planeja usar o Citrix Managed Azure, certifique-se de solicitar o Citrix Azure Consumption Fund (além do Citrix DaaS), por meio do Citrix ou do Azure Marketplace.

- **Licenciamento do Windows:** verifique se você está devidamente licenciado para que os Serviços de Área de Trabalho Remota executem cargas de trabalho do Windows Server ou Licenciamento de Área de Trabalho Virtual do Azure para Windows 10 Para obter mais informações, consulte Configurar um servidor de licenças do Microsoft RDS.
- Se você planeja usar uma assinatura do Citrix Managed Azure e deseja unir VDAs a um domínio usando a Política de Grupo do Active Directory, você deve ser um administrador com permissão para executar essa ação no Active Directory. Para obter detalhes, consulte Responsabilidade do cliente.
- Configurar conexões com sua rede local corporativa tem requisitos extras.
  - Qualquer conexão (Azure VNet peering ou SD-WAN): Requisitos para todas as conexões.
  - Conexões de peering do Azure VNet: requisitos e preparação de peering do VNet.
  - Conexões SD-WAN: requisitos e preparação da conexão SD-WAN.
- Se você planeja usar suas próprias imagens do Azure ao criar um catálogo, essas imagens devem atender a determinados requisitos.
- Requisitos de conectividade com a Internet: Requisitos de sistema e conectividade.
- Limites de recursos em uma implantação do Citrix DaaS: limites.

Sistemas operacionais compatíveis

Ao usar o Quick Deploy com uma assinatura do Citrix Managed Azure:

- Windows 10 de sessão única
- Windows 10 multissessão
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

- Red Hat Enterprise Linux e Ubuntu

Ao usar o Quick Deploy com uma assinatura do Azure gerenciada pelo cliente:

- Windows 10 Enterprise de sessão única
- Área de trabalho virtual do Windows 10 Enterprise multissessão
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux e Ubuntu

Configure uma rápida implantação de prova de conceito

Esse procedimento requer uma assinatura do Citrix Managed Azure.

1. Criar um catálogo usando a criação rápida.
2. Adicionar seus usuários ao Managed Azure AD.
3. Adicionar seus usuários ao catálogo.
4. Notificar seus usuários sobre a URL do espaço de trabalho.

Configurar uma implantação de produção

1. Se você estiver usando seu próprio Active Directory ou Azure Active Directory para autenticar usuários, conecte-se e defina esse método no Citrix Cloud.
2. Se você estiver usando máquinas ingressadas no domínio, confirme se você tem entradas válidas de servidor DNS.
3. Se você estiver usando sua própria assinatura do Azure (em vez de uma assinatura do Citrix Managed Azure), adicione sua assinatura do Azure.
4. Criar ou importe uma imagem. Embora você possa usar uma das imagens preparadas pela Citrix no estado em que se encontram em um catálogo, elas se destinam principalmente a implantações de prova de conceito.
5. Se você estiver usando uma assinatura do Citrix Managed Azure e quiser que seus usuários possam acessar itens em sua rede (como servidores de arquivos), configure um emparelhamento VNet do Azure ou uma conexão Citrix SD-WAN.
6. Criar um catálogo usando a criação personalizada.

7. Se você estiver criando um catálogo de máquinas com várias sessões, adicionar aplicativos ao catálogo, se necessário.
8. Se você estiver usando o Citrix Managed Azure AD para autenticar seus usuários, adicionar usuários ao diretório.
9. Adicione usuários ao catálogo.
10. Notificar seus usuários sobre a URL do espaço de trabalho.

Depois de configurar a implantação, use o painel **Quick Deploy > Monitor** para ver o uso da área de trabalho, sessões e máquinas.

URL do Workspace

Depois de criar catálogos e atribuir usuários, notifique os usuários sobre onde encontrar suas áreas de trabalho e aplicativos: a URL do espaço de trabalho. A URL do espaço de trabalho é a mesma para todos os catálogos e usuários.

A URL do espaço de trabalho está disponível em dois locais:

- Em **Manage > Quick Deploy** no Citrix DaaS, visualize o URL expandindo **User Access & Authentication** à direita.
- No console do Citrix Cloud, selecione **Workspace Configuration** no menu no canto superior esquerdo. A guia **Access** contém a URL do Workspace.

Para obter informações sobre como personalizar a URL do espaço de trabalho, consulte Customize the Workspace URL.

Depois que os usuários navegam até a URL do Workspace e se autenticam, eles podem iniciar suas áreas de trabalho e aplicativos.

Obtenha ajuda

- Leia o artigo Troubleshoot.
- Se você ainda tiver problemas com o Citrix DaaS, abra um ticket seguindo as instruções em How to Get Help and Support.

Imagens no Quick Deploy

Quando você cria um catálogo para fornecer áreas de trabalho ou aplicativos, uma imagem é usada (com outras configurações) como um modelo para criar as máquinas.

O Quick Deploy fornece um conjunto de imagens preparadas que você pode escolher para criar e personalizar uma imagem no Quick Deploy. Você também pode importar (adicionar) e usar imagens de suas próprias assinaturas do Azure.

Imagens preparadas pela Citrix

O Quick Deploy fornece várias imagens preparadas pela Citrix:

- Windows 10 Enterprise (sessão única)
- Área de trabalho virtual do Windows 10 Enterprise (multissessão)
- Área de Trabalho Virtual do Windows 10 Enterprise (multissessão) com o Office 365 ProPlus
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Linux Ubuntu (sessão única e multissessão)

As imagens preparadas pela Citrix têm um Citrix Virtual Delivery Agent (VDA) atual e ferramentas de solução de problemas instaladas. O VDA é o mecanismo de comunicação entre as máquinas dos usuários e a infraestrutura do Citrix Cloud que gerencia o Citrix DaaS (antigo serviço Citrix Virtual Apps and Desktops). As imagens fornecidas pela Citrix têm uma notação **CITRIX** .

As imagens preparadas pela Citrix não estão disponíveis na interface Full Configuration do Citrix DaaS.

Você também pode importar e usar sua própria imagem do Azure.

Maneiras de usar imagens no Quick Deploy

Você pode:

- **Use a Citrix prepared image when creating a catalog.** Essa opção é recomendada somente para implantações de prova de conceito.
- **Use a Citrix prepared image to create another image.** Depois que a nova imagem é criada, você a personaliza adicionando aplicativos e outros softwares de que seus usuários precisam. Em seguida, você pode usar essa imagem personalizada ao criar um catálogo.
- **Import an image from Azure.** Depois de importar uma imagem do Azure, você pode usar essa imagem ao criar um catálogo.

Ou você pode usar essa imagem para criar uma nova imagem e personalizá-la adicionando aplicativos. Em seguida, você pode usar essa imagem personalizada ao criar um catálogo.

Quando você cria um catálogo, o Citrix DaaS verifica se a imagem usa um sistema operacional válido e tem um Citrix VDA e ferramentas de solução de problemas instaladas (junto com outras verificações).

Exibir informações da imagem

1. Em **Manage > Quick Deploy**, expanda **Master Images** à direita. A tela lista as imagens preparadas pela Citrix e todas as imagens importadas.

2. Selecione uma imagem para exibir seus detalhes.

   No cartão de detalhes, você pode:

   - Alterar (editar) o nome da imagem.
   - Adicionar e editar notas (disponível apenas para imagens que você preparou ou importou, não para imagens preparadas pela Citrix).
   - Excluir a imagem.

Preparar uma nova imagem

Preparar uma nova imagem inclui a criação e personalização da imagem. Quando você cria uma imagem, uma nova VM é criada para carregar a nova imagem.

Requisitos:

- Conheça as características de desempenho de que as máquinas precisam. Por exemplo, a execução de aplicativos CAD pode exigir CPU, RAM e armazenamento diferentes dos outros aplicativos de escritório.
- Se você planeja usar uma conexão com seus recursos locais, configure essa conexão antes de criar a imagem e o catálogo. Para obter detalhes, consulte Network connections.

Ao usar uma imagem do Ubuntu preparada pela Citrix para criar uma nova imagem, é criada uma senha root para a nova imagem. Você pode alterar essa senha de root, mas somente durante o processo de criação e personalização da imagem. (Você não pode alterar a senha root depois que a imagem for usada em um catálogo.)

- Quando a imagem é criada, a conta de administrador que você especificou (**Login details for image building machine**) é adicionada ao grupo `sudoers`.
- Depois de fazer o RDP para a máquina que contém a nova imagem, inicie o aplicativo de terminal e digite `sudo passwd root`. Quando solicitado, forneça a senha especificada ao criar a imagem. Após a verificação, você será solicitado a inserir uma nova senha para o usuário root.

Para criar uma imagem:

1. Em **Manage > Quick Deploy**, expanda **Master Images** à direita.
2. Selecione **Build Image**.

3. Insira valores nos seguintes campos:

   - **Name:** insira um nome para a nova imagem.
   - **Master image:** selecione uma imagem existente. Essa é a imagem base usada para criar a nova imagem.
   - **Subscription:** selecione uma assinatura do Azure.
   - **Network connection:**
     - Se estiver usando uma assinatura do Citrix Managed Azure, selecione **No connectivity** ou uma conexão criada anteriormente.
     - Se estiver usando sua própria assinatura do Azure gerenciada pelo cliente, selecione seu grupo de recursos, rede virtual e sub-rede. Em seguida, adicione os detalhes do domínio: FQDN, OU, nome da conta Citrix DaaS e credenciais.
   - **Region:** (disponível somente para **No connectivity**.) Selecione uma região onde você deseja que a máquina que contém a imagem seja criada.
   - **Logon credentials for image machine:** você usará essas credenciais mais tarde quando se conectar (RDP) à máquina que contém a nova imagem, para que você possa instalar aplicativos e outros softwares.
   - **Machine performance:** são informações de CPU, RAM e armazenamento da máquina que executa a imagem. Selecione um desempenho de máquina que atenda aos requisitos dos seus aplicativos.

- **Restricted IP access:** se você quiser restringir o acesso a endereços específicos, selecione **Add IP addresses** e insira um ou mais endereços. Depois de adicionar os endereços, selecione **Done** para retornar ao cartão **Build image** .
- **Notes:** opcionalmente, adicione até 1024 caracteres de notas. Depois que a imagem é criada, você pode atualizar as notas na exibição de detalhes da imagem.
- **Local domain join:** indique se você deseja ingressar no domínio local do Active Directory.
  - Se você selecionar **Yes**, insira o FQDN, a OU, o nome da conta do Citrix DaaS e as credenciais.
  - Se você selecionar **No**, insira as credenciais da máquina host.

4. Quando terminar, selecione **Build Image**.

Uma imagem pode levar até 30 minutos para ser criada. Em **Manage > Quick Deploy**, expanda **Master Images** à direita para ver o estado atual (como `Building image` ou `Ready to customize`).

O que fazer a seguir: conectar-se a uma nova imagem e personalizá-la.

Conectar-se a uma nova imagem e personalizá-la

Depois que uma nova imagem é criada, seu nome é adicionado à lista de imagens, com um status de `Ready to customize` (ou alguma expressão semelhante). Para personalizar essa imagem, primeiro faça o download de um arquivo RDP. Ao usar esse arquivo para se conectar à imagem, você pode adicionar aplicativos e outros softwares à imagem.

1. Em **Manage > Quick Deploy**, expanda **Master Images** à direita. Selecione a imagem à qual você deseja se conectar.
2. Selecione **Download RDP file**. É feito o download de um cliente RDP.

   A máquina de imagem pode se desligar se você não fizer uma conexão por RDP a ela logo após sua criação. Isso economiza custos. Quando isso acontecer, selecione **Power On**.
3. Inicie o cliente RDP baixado. Ele tenta se conectar automaticamente ao endereço da máquina que contém a nova imagem. Quando solicitado, insira as credenciais especificadas ao criar a imagem.
4. Depois de se conectar à máquina, adicione ou remova aplicativos, instale atualizações e conclua qualquer outro trabalho de personalização.

   NÃO aplique Sysprep à imagem.

5. Quando terminar de personalizar a nova imagem, retorne à caixa **Master Images** e selecione **Finish build**. A nova imagem passa automaticamente por testes de validação.

Posteriormente, quando você cria um catálogo, a nova imagem é incluída na lista de imagens que você pode selecionar.

Em **Manage > Quick Deploy**, a exibição da imagem à direita indica quantos catálogos e máquinas usam cada imagem.

> **Nota:**
>
> Depois de finalizar uma imagem, você não poderá editá-la. Você deve criar uma nova imagem (opcionalmente usando a imagem anterior como ponto de partida) e, em seguida, atualizar a nova imagem.

Importar uma imagem do Azure

Ao importar uma imagem do Azure que tenha um Citrix VDA e aplicativos de que seus usuários precisam, você pode usá-la para criar um catálogo ou substituir a imagem em um catálogo existente.

Requisitos de imagem importada

> **Nota:**
>
> O Citrix DaaS não oferece suporte à importação de discos associados às VMs da geração 2 do Azure.

> A Citrix executa testes de validação na imagem importada. Os seguintes requisitos devem ser atendidos ao preparar a imagem que você importará para o Citrix DaaS.

- **Supported OS:** a imagem deve ser um sistema operacional com suporte. Para verificar uma versão do sistema operacional Windows, execute `Get-WmiObject Win32_OperatingSystem`.
- **Supported generation:** somente VMs de geração 1 têm suporte.
- **Not generalized:** a imagem não deve ser generalizada.

- **No configured Delivery Controllers:** nenhum Citrix Delivery Controller deve estar configurado na imagem. As chaves de registro a seguir devem estar limpas.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Personality.ini file:** o arquivo `personality.ini` deve existir na unidade do sistema.
- **Valid VDA:** a imagem deve ter um Citrix VDA mais recente que 7.11 instalado.
  - Windows: Para verificar, use `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. Para obter orientações sobre instalação, consulte Instalar um VDA do Windows em uma imagem.
  - Red Hat Enterprise Linux e Ubuntu: Para obter orientações de instalação, consulte a documentação do produto.
- **Azure Virtual Machine Agent:** Antes de importar uma imagem, verifique se o Azure Virtual Machine Agent está instalado na imagem. Para obter mais informações, consulte o artigo da Microsoft Visão geral do Azure Virtual Machine Agent.

Importe a imagem usando Quick Deploy

1. Em **Manage > Quick Deploy**, expanda **Master Images** à direita.

2. Selecione **Import Image**.

3. Escolha como importar a imagem.
   - No caso de discos gerenciados, use o recurso de exportação para gerar um URL de SAS. Defina o tempo de expiração como 7200 segundos ou mais.
   - No caso de VHDs em uma conta de armazenamento, escolha uma das seguintes opções:
     - Gerar um URL SAS para o arquivo VHD.
     - Atualizar o nível de acesso de um contêiner de armazenamento em bloco para blob ou contêiner. Em seguida, obtenha o URL do arquivo.

4. Se você selecionou **Browse storage account**:
    a. Selecione sequencialmente uma assinatura > grupo de recursos > conta de armazenamento > imagem.
    b. Dê um nome à imagem.
5. Se você selecionou a **Azure public URL**:
    a. Insira o URL gerado pelo Azure para o VHD. Para obter orientação, selecione o link para o documento da Microsoft Download a Windows VHD from Azure.
    b. Selecione uma assinatura (Uma imagem do Linux só pode ser importada se você selecionar uma assinatura gerenciada pelo cliente.)
    c. Dê um nome à imagem.
6. Quando terminar, selecione **Import Image**.

Atualizar um catálogo de Quick Deploy com uma nova imagem

O tipo de catálogo determina quais máquinas são atualizadas quando você atualiza o catálogo.

- No caso de um catálogo aleatório, todas as máquinas atualmente no catálogo são atualizadas com a imagem mais recente. Se você adicionar mais áreas de trabalho a esse catálogo, elas serão baseadas na imagem mais recente.
- No caso de um catálogo estático, as máquinas atualmente no catálogo não são atualizadas com a imagem mais recente. As máquinas atualmente contidas no catálogo continuam usando a imagem a partir da qual foram criadas. No entanto, se você adicionar mais máquinas a esse catálogo, elas serão baseadas na imagem mais recente.

Você pode atualizar um catálogo contendo máquinas com imagens gen1 com uma imagem gen2, se as máquinas do catálogo suportarem gen2. Da mesma forma, você pode atualizar um catálogo contendo máquinas gen2 com uma imagem gen1, se as máquinas do catálogo oferecerem suporte a gen1.

Para atualizar um catálogo com uma nova imagem:

1. Em **Manage > Quick Deploy**, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Details**, selecione **Update Image**.



3. Selecione uma imagem.

4. No caso de catálogos aleatórios ou de várias sessões: selecione um intervalo de logoff. Depois que o Citrix DaaS concluir o processamento inicial da imagem, os assinantes recebem um aviso para salvar seu trabalho e fazer logoff de seus desktops. O intervalo de logoff indica quanto tempo os assinantes têm depois de receber a mensagem até que a sessão termine automaticamente.
5. Selecione **Update Image**.

Excluir uma imagem do Quick Deploy

1. Em **Manage > Quick Deploy**, expanda **Master Images** à direita.
2. Selecione a imagem que você deseja excluir.
3. Selecione **Delete Image** na parte inferior do cartão. Confirme a exclusão.

Instalar um VDA do Windows em uma imagem

Use o procedimento a seguir ao preparar uma imagem do Windows que você planeja importar para o Citrix DaaS.

Para obter orientações sobre a instalação do Linux VDA, consulte a documentação do produto Linux VDA.

1. No seu ambiente do Azure, conecte-se à VM de imagem (se você ainda não estiver conectado).
2. Você pode baixar um VDA usando o link **Downloads** na barra de navegação do Citrix Cloud. Ou use um navegador para navegar até a página de download do Citrix DaaS.

   Faça o download de um VDA na VM. Existem pacotes de download de VDA separados para um sistema operacional de desktop (sessão única) e um sistema operacional de servidor (multissessão).
3. Inicie o instalador do VDA clicando duas vezes no arquivo baixado. O assistente de instalação é iniciado.
4. Na página **Environment**, selecione a opção para criar uma imagem usando o MCS e, em seguida, selecione **Next**.
5. Na página **Core Components**, selecione **Next**.
6. Na página **Delivery Controller**, selecione **Let Machine Creation Services do it automatically** e, em seguida, selecione **Next**. Confirme sua seleção, se solicitado.
7. Deixe as configurações padrão nas páginas **Additional Components**, **Features** e **Firewall**, a menos que a Citrix dê instruções diferentes. Selecione **Next** em cada página.

8. Na página **Summary**, selecione **Install**. Os pré-requisitos começam a ser instalados. Quando solicitado a reiniciar, concorde.
9. A instalação do VDA é retomada automaticamente. A instalação de pré-requisito é concluída e, em seguida, os componentes e recursos são instalados. Na página **Call Home**, deixe a configuração padrão (a menos que a Citrix o instrua de outra forma). Depois de se conectar, selecione **Next**.
10. Selecione **Finish**. A máquina reinicia automaticamente.
11. Para garantir que a configuração esteja correta, inicie um ou mais dos aplicativos que você instalou na VM.
12. Desligue a VM. Não aplique Sysprep à imagem.

Para obter mais informações sobre a instalação de VDAs, consulte Install VDAs.

Monitorar no Quick Deploy

No painel **Monitor**, você pode visualizar o uso da área de trabalho, as sessões e as máquinas na implantação do Citrix DaaS (antigo serviço Citrix Virtual Apps and Desktops). Você também pode controlar sessões, gerenciar a energia de máquinas, finalizar aplicativos em execução e finalizar processos em execução.

Para acessar o painel **Monitor** :

1. Faça logon no Citrix Cloud, caso ainda não tenha feito. No menu superior esquerdo, selecione **My Services > DaaS**.
2. No painel **Manage > Quick Deploy**, selecione a guia **Monitor** .

Monitore o uso de áreas de trabalho

As exibições nesta página são atualizadas a cada cinco minutos.

- **Visão geral da máquina e das sessões:** Você pode personalizar a exibição para mostrar informações sobre todos os catálogos (padrão) ou um catálogo selecionado. Você também pode personalizar o período de tempo: o último dia, semana, mês ou três meses.

  As contagens na parte superior do display indicam o número total de máquinas, mais o número de máquinas que estão ligadas e desligadas. Passe o mouse sobre um valor para exibir quantas são de sessão única e de várias sessões.

O gráfico abaixo das contagens mostra o número de máquinas ligadas e picos de sessões simultâneas em pontos regulares durante o período selecionado. Passe o mouse sobre um ponto do gráfico para exibir as contagens nesse ponto.



- **Top 10s:** para personalizar uma exibição dos 10 principais, selecione um período de tempo: a semana passada (padrão), mês ou três meses. Você também pode personalizar a exibição para mostrar somente informações sobre atividades envolvendo máquinas de sessão única, máquinas com várias sessões ou aplicativos.
  - **Top 10 Active Users:** lista os usuários que iniciaram desktops com mais frequência durante o período. Passar o mouse sobre uma linha exibe o total de inicializações.
  - **Top 10 Active Catalogs:** lista os catálogos com maior duração durante o período selecionado. A duração é a soma de todas as sessões do usuário desse catálogo.

Relatório de uso de desktop

Para baixar um relatório contendo informações sobre inicializações de máquinas durante o último mês, selecione **Launch Activity**. Uma mensagem indica que a solicitação está sendo processada. O relatório é baixado automaticamente para o local de download padrão na máquina local.

Filtre e pesquise para monitorar máquinas e sessões

Quando você está monitorando as informações da sessão e da máquina, todas as máquinas ou sessões são exibidas por padrão. Você pode:

- Filtrar a exibição por máquinas, sessões, conexões ou aplicativos.
- Refinar a exibição de sessões ou máquinas escolhendo os critérios desejados, criando um filtro usando expressões.
- Salvar os filtros que você cria para reutilização.

Controlar os aplicativos de um usuário

Você pode exibir e gerenciar aplicativos e processos para um usuário que tenha uma sessão em execução ou uma área de trabalho atribuída.

1. No painel **Monitor** no Citrix DaaS, selecione **Search** e insira o nome do usuário (ou os caracteres iniciais do nome do usuário), a máquina ou o endpoint. Nos resultados da pesquisa, selecione o item que você está procurando. (Para recolher a caixa de pesquisa sem pesquisar, selecione **Search** novamente.)

2. Selecione uma sessão.

   O Gerenciador de atividades lista os aplicativos e processos para a sessão do usuário.
3. Para finalizar um aplicativo, na guia **Applications** no Gerenciador de atividades, selecione na linha do aplicativo para selecionar esse aplicativo e, em seguida, selecione **End Application**.

   
4. Para finalizar um processo, na guia **Processes** no Activity Manager, selecione na linha do processo para selecionar esse processo e, em seguida, selecione **End Process**.
5. Para exibir os detalhes da sessão, selecione **Details** no canto superior direito. Para retornar à exibição de aplicativos e processos, selecione Activity Manager no canto superior direito.
6. Para controlar a sessão, selecione **Session Control > Log Off** ou **Session Control > Disconnect**.

Sombrear usuários

Use o recurso de sombreamento para exibir ou trabalhar diretamente na sessão ou na máquina virtual de um usuário. Você pode sombrear VDAs Windows e Linux. O usuário deve estar conectado à máquina que você deseja sombrear. Para confirmar essa conexão, verifique o nome da máquina listado na barra de título `User`.

O sombreamento é iniciado em uma nova guia do navegador. O seu navegador deve permitir pop-ups do URL do Citrix Cloud.

O sombreamento é suportado somente para usuários em máquinas ingressadas no domínio. Para sombrear uma máquina não ingressada no domínio, você deve configurar uma máquina bastion. Para obter detalhes, consulte Bastion access.

O sombreamento deve ser iniciado a partir de uma máquina na mesma rede virtual que as máquinas ingressadas no domínio e também atender aos requisitos de porta.

Habilitar sombreamento

1. Em **Manage > Quick Deploy > Monitor**, acesse a visualização **User Details** .
2. Selecione a sessão do usuário e selecione **Shadow** na exibição do **Activity Manager** ou no painel **Session Details**.

VDAs Linux sombra

O sombreamento, ou shadowing, está disponível para Linux VDAs versão 7.16 ou posterior executando as distribuições Linux RHEL7.3 ou Ubuntu versão 16.04

O Monitor usa o FQDN para se conectar ao Linux VDA de destino. É preciso que o Monitor cliente possa resolver o FQDN do Linux VDA.

- O VDA deve ter os pacotes `python-websockify` e `x11vn` instalados.
- A conexão `noVNC` com o VDA usa o protocolo WebSocket. Por padrão, é usado o protocolo WebSocket `ws://`. Por motivos de segurança, a Citrix recomenda que você use o protocolo seguro `wss://`. Instale certificados SSL em cada cliente do Monitor e Linux VDA.

Siga as instruções em Session Shadowing para configurar seu VDA Linux para sombreamento.

1. Depois que você ativar o sombreamento, a conexão de sombreamento é inicializada e um prompt de confirmação aparece no dispositivo do usuário.
2. Instrua o usuário a clicar em **Yes** para iniciar a máquina ou o compartilhamento de sessão.
3. O administrador só pode visualizar a sessão sombreada.

VDAs do Windows sombra

As sessões do Windows VDA são sombreadas usando a Assistência Remota do Windows. Ative o recurso `Use Windows Remote Assistance` ao instalar o VDA.

1. Depois de habilitar o sombreamento, a conexão de sombreamento é inicializada e uma caixa de diálogo solicita que você abra ou salve o arquivo `.msrc incident`.
2. Abra o arquivo de incidente com o Visualizador de Assistência Remota, se ainda não estiver selecionado por padrão. Um prompt de confirmação é exibido no dispositivo do usuário.
3. Instrua o usuário a clicar em **Yes** para iniciar a máquina ou o compartilhamento de sessão.
4. Para obter mais controle, peça ao usuário que compartilhe o controle do teclado e do mouse.

Monitorar e controlar sessões

A exibição da sessão são atualizadas a cada minuto.

Além de ver sessões, você pode desconectar uma ou mais sessões ou desconectar usuários das sessões.

1. Em **Manage > Quick Deploy > Monitor**, selecione **Filters**.

2. Selecione a visualização **Sessions** .
3. Para personalizar a exibição, selecione **Choose Columns** e marque as caixas de seleção dos itens que deseja que apareçam. Quando terminar, selecione **OK**. A exibição das sessões é atualizada automaticamente.
4. Marque a caixa de seleção à esquerda de cada sessão que você deseja controlar.
5. Para fazer logoff ou desconectar a sessão, selecione **Session Control > Log Off** ou **Session Control > Disconnect**.

Lembre-se de que a programação de gerenciamento de energia para o catálogo também pode controlar a desconexão de sessões e o logoff de usuários de sessões desconectadas.

Como alternativa ao procedimento acima, você também pode **Pesquisar** um usuário, selecionar a sessão que deseja controlar e, em seguida, exibir os detalhes da sessão. Ali, as opções de logoff e desconexão também estão disponíveis.

Relatório de informações da sessão

Para baixar as informações da sessão, selecione **Exportar** na exibição das sessões. Uma mensagem indica que a solicitação está sendo processada. O relatório é baixado automaticamente para o local de download padrão na máquina local.

Máquinas de monitoramento e controle de energia

Os visores da máquina são atualizados a cada minuto.

1. Em **Manage > Quick Deploy > Monitor**, selecione **Filters**.
2. Selecione a visualização **Machines** .

   Por padrão, a tela lista máquinas com sistema operacional de sessão única. Como alternativa, você pode exibir máquinas com multissessão.
3. Para personalizar a exibição, selecione **Choose Columns** e marque as caixas de seleção dos itens que deseja que apareçam. Quando terminar, selecione **OK**. As máquinas exibem atualizações automaticamente.

4. Para controlar as máquinas ou colocá-las dentro ou fora do modo de manutenção, marque a caixa de seleção à esquerda de cada máquina que você deseja controlar.
5. Para controlar a potência das máquinas selecionadas, selecione **Power Control** e selecione uma ação.

6. Para colocar as máquinas selecionadas dentro ou fora do modo de manutenção, selecione **Maintenance Mode > ON** ou **Maintenance Mode > OFF**.

Ao usar o recurso de pesquisa para localizar e selecionar uma máquina, você vê detalhes da máquina, utilização, histórico de utilização (dos últimos sete dias) e IOPS médio.

Relatório de informações da máquina

Para baixar as informações da sessão, selecione **Export** na tela da máquina. Uma mensagem indica que a solicitação está sendo processada. O relatório é baixado automaticamente para o local de download padrão na máquina local.

Verificação da integridade de aplicativos e desktops

A investigação automatiza o processo de verificação da integridade de aplicativos e desktops publicados. Os resultados da verificação de integridade estão disponíveis no painel **Monitor** \. Para obter detalhes, consulte:

- Investigação de aplicativo
- Investigação da área de trabalho

Conexões de rede no Quick Deploy

Introdução

Este artigo fornece detalhes sobre como criar conexões de rede para seus recursos corporativos ao usar uma assinatura do Citrix Managed Azure.

Ao usar sua própria assinatura do Azure gerenciada pelo cliente, não há necessidade de criar uma conexão de rede.

Ao criar um catálogo de Quick Deploy, você indica se e como os usuários acessam locais e recursos em sua rede local corporativa a partir de seus desktops e aplicativos Citrix. Ao usar uma conexão, você deve criar a conexão antes de criar o catálogo.

Ao usar uma assinatura do Citrix Managed Azure, as opções são:

- Sem conectividade
- Emparelhamento do Azure VNet
- SD-WAN

Não é possível alterar o tipo de conexão de um catálogo após a criação desse catálogo.

Requisitos para todas as conexões de rede

- Ao criar uma conexão, você deve ter entradas de servidor DNS válidas.
- Ao usar o Secure DNS ou um provedor de DNS de terceiros, você deve adicionar o intervalo de endereços alocado para uso pelo Citrix DaaS (antigo serviço Citrix Virtual Apps and Desktops) aos endereços IP do provedor de DNS na lista de permissões. Esse intervalo de endereços é especificado quando você cria uma conexão.
- Todos os recursos de serviço que usam a conexão (máquinas ingressadas no domínio) devem ser capazes de acessar seu servidor NTP (Network Time Protocol), para garantir a sincronização de horário.

Sem conectividade

Quando um catálogo é configurado com **Sem conectividade**, os usuários não podem acessar recursos em suas redes locais ou em outras redes. Essa é a única opção ao criar um catálogo usando a criação rápida.



Sobre as conexões emparelhadas do Azure VNet

O peering de rede virtual conecta perfeitamente duas redes virtuais do Azure (VNets): a sua e o Citrix DaaS VNet. O emparelhamento também ajuda a permitir que os usuários acessem arquivos e outros itens de suas redes locais.

Conforme mostrado no gráfico a seguir, você cria uma conexão usando o emparelhamento VNet do Azure da assinatura do Citrix Managed Azure para o VNet na assinatura do Azure da sua empresa.



Aqui está outra ilustração do emparelhamento VNet.



Os usuários podem acessar seus recursos de rede (como servidores de arquivos) ingressando no domínio local quando você cria um catálogo. (Ou seja, você ingressa no domínio do AD onde residem compartilhamentos de arquivos e outros recursos necessários.) Sua assinatura do Azure se conecta a esses recursos (nos gráficos, usando uma VPN ou o Azure ExpressRoute). Ao criar o catálogo, você fornece o domínio, a UO e as credenciais da conta.

> **Importante:**
>
> - Saiba mais sobre o emparelhamento do Azure VNet antes de usá-lo neste serviço.
> - Crie uma conexão de emparelhamento VNet antes de criar um catálogo que a use.

Rotas personalizadas de peering do Azure VNet

As rotas personalizadas ou definidas pelo usuário substituem as rotas do sistema padrão do Azure para direcionar o tráfego entre máquinas virtuais em um emparelhamento VNet, redes locais e a Internet. Você pode usar rotas personalizadas se houver redes que se espera que os recursos do Citrix DaaS acessem, mas não estejam diretamente conectadas por meio de emparelhamento de VNet. Por exemplo, você pode criar uma rota personalizada que force o tráfego através de um dispositivo de rede para a Internet ou para uma sub-rede de rede local.

Para usar rotas personalizadas:

- Você deve ter um gateway de rede virtual do Azure existente ou um dispositivo de rede como o Citrix SD-WAN em seu ambiente Citrix DaaS.
- Ao adicionar rotas personalizadas, você deve atualizar as tabelas de rotas da sua empresa com as informações VNet de destino do Citrix DaaS para garantir a conectividade de ponta a ponta.
- As rotas personalizadas são exibidas no Citrix DaaS na ordem em que são inseridas. Essa ordem de exibição não afeta a ordem na qual o Azure seleciona rotas.

Antes de usar rotas personalizadas, consulte o artigo da Microsoft Virtual network traffic routing para saber mais sobre como usar rotas personalizadas, tipos de salto seguinte e como o Azure seleciona rotas para tráfego de saída.

Você pode adicionar rotas personalizadas ao criar uma conexão de emparelhamento do Azure VNet ou para as existentes em seu ambiente Citrix DaaS. Quando você estiver pronto para usar rotas personalizadas com seu emparelhamento de VNet, consulte as seções a seguir neste artigo:

- Para rotas personalizadas com novos peerings do Azure VNet: Create an Azure VNet peering connection
- Para rotas personalizadas com peerings de VNet do Azure existentes: Manage custom routes for existing Azure VNet peer connections

Requisitos e preparação de peering do Azure VNet

- Credenciais para um proprietário da assinatura do Azure. Essa deve ser uma conta do Azure Active Directory. Este serviço não oferece suporte a outros tipos de conta, como live.com ou contas externas do Azure AD (em um locatário diferente).
- Uma assinatura do Azure, um grupo de recursos e uma rede virtual (VNet).
- Configure as rotas de rede do Azure para que os VDAs na assinatura do Citrix Managed Azure possam se comunicar com seus locais de rede.
- Abra os grupos de segurança de rede do Azure da sua VNet para o intervalo de IP especificado.
- **Active Directory:** em cenários de ingresso em domínios, recomendamos que você tenha alguma forma de serviços do Active Directory em execução na VNet emparelhada. Isso aproveita as características de baixa latência da tecnologia de emparelhamento VNet do Azure.

  Por exemplo, a configuração pode incluir os Serviços de Domínio do Azure Active Directory (AADDS), uma VM de controlador de domínio na VNet ou o Azure AD Connect ao Active Directory local.

  Depois de habilitar o AADDS, você não poderá mover seu domínio gerenciado para uma VNet diferente sem excluir o domínio gerenciado. Portanto, é importante selecionar a VNet correta para habilitar seu domínio gerenciado. Antes de continuar, leia o artigo da Microsoft Networking considerations for Azure AD Domain Services.
- **VNet IP range:** ao criar a conexão, você deve fornecer um espaço de endereço CIDR disponível (endereço IP e prefixo de rede) que seja exclusivo entre os recursos de rede e as VNets do Azure conectadas. Esse é o intervalo de IP atribuído às VMs dentro da VNet emparelhada do Citrix DaaS.

  Lembre-se de especificar um intervalo de IP que não se sobreponha a nenhum endereço usado em suas redes do Azure e locais.

  - Por exemplo, se sua VNet do Azure tiver um espaço de endereço de 10.0.0.0 /16, crie a conexão de emparelhamento VNet no Citrix DaaS como algo como 192.168.0.0 /24.

- Neste exemplo, criar uma conexão de peering com um intervalo de IP 10.0.0.0 /24 seria considerado um intervalo de endereços sobreposto.

Se os endereços se sobrepuserem, poderá não ser possível criar a conexão de emparelhamento VNet. Também não funciona corretamente para tarefas de administração do site.

Para saber mais sobre o emparelhamento de VNet, consulte os seguintes artigos da Microsoft.

- Virtual network peering
- Azure VPN Gateway
- Create a Site-to-Site connection in the Azure portal
- VPN Gateway FAQ (procure por "overlap")

Criar uma conexão emparelhada do Azure VNet

1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita. Se você já tiver configurado conexões, elas estão listadas.

2. Selecione **Add Connection**.
3. Clique em qualquer lugar na caixa **Add Azure VNet Peering** .

4. Selecione **Authenticate Azure Account**.

5. O Citrix DaaS leva você automaticamente para a página de login do Azure para autenticar suas assinaturas do Azure. Depois de entrar no Azure (com as credenciais da conta de administrador global) e aceitar os termos, você retornará à caixa de diálogo de detalhes da criação da conexão.

6. Digite um nome para o par VNet do Azure.
7. Selecione a assinatura do Azure, o grupo de recursos e o VNet to peer.
8. Indique se a VNet selecionada usa um Gateway de Rede Virtual do Azure. Para obter informações, consulte o artigo da Microsoft Azure VPN Gateway.

9. Se você respondeu **Yes** na etapa anterior (a VNet usa um gateway de rede virtual do Azure), indique se deseja habilitar a propagação de rota do gateway de rede virtual. Quando habilitado, o Azure aprende (adiciona) automaticamente todas as rotas por meio do gateway.

   Você pode alterar essa configuração posteriormente na página **Details** da conexão. No entanto, essa alteração pode causar alterações no padrão de rota e interrupções de tráfego VDA. Além disso, se você a desativar posteriormente, deverá adicionar manualmente as rotas às redes que os VDAs usarão.

10. Digite um endereço IP e selecione uma máscara de rede. O intervalo de endereços a ser usado é exibido, além de quantos endereços o intervalo suporta. Certifique-se de que o intervalo de IP não se sobreponha a nenhum endereço usado em suas redes locais e do Azure.

    - Por exemplo, se sua VNet do Azure tiver um espaço de endereço de 10.0.0.0 /16, crie a conexão de emparelhamento VNet no Citrix DaaS como algo como 192.168.0.0 /24.
    - Neste exemplo, a criação de uma conexão de emparelhamento VNet com um intervalo de IP 10.0.0.0 /24 é considerada um intervalo de endereços sobreposto.

    Se os endereços se sobrepuserem, poderá não ser possível criar a conexão de emparelhamento VNet. Também não funciona corretamente para tarefas de administração do site.

11. Indique se você deseja adicionar rotas personalizadas à conexão de emparelhamento VNet. Se selecionar **Yes**, insira as seguintes informações:

    a. Digite um nome amigável para a rota personalizada.

    b. Insira o endereço IP de destino e o prefixo da rede. O prefixo da rede deve estar entre 16 e 24.

    c. Selecione um tipo de próximo salto para onde você deseja que o tráfego seja roteado. Se você selecionar **Virtual appliance**, digite o endereço IP interno do equipamento.

    ▢

    Para obter mais informações sobre os tipos de salto seguinte, consulte a seção Custom routes no artigo da Microsoft *Virtual network traffic routing*.

    d. Para criar outra rota personalizada para a conexão, selecione **Add route**.

12. Selecione **Add VNet Peering**.

Depois que a conexão é criada, ela é listada em **Network Connections > Azure VNet Peers** no lado direito do painel **Manage > Quick Deploy** \. Quando você cria um catálogo, essa conexão é incluída na lista de conexões de rede disponíveis.

Veja os detalhes da conexão de peering do Azure VNet

1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita.
2. Selecione a conexão emparelhada do Azure VNet que você deseja exibir.

Os detalhes incluem:

- O número de catálogos, máquinas, imagens e bastions que usam essa conexão.
- A região, o espaço de rede alocado e as VNets emparelhadas.
- As rotas atualmente configuradas para a conexão de emparelhamento VNet.

Gerenciar rotas personalizadas para conexões de mesmo nível existentes do Azure VNet

Você pode adicionar novas rotas personalizadas a uma conexão existente ou modificar rotas personalizadas existentes, inclusive a desativação ou exclusão de rotas personalizadas.

> **Importante:**
>
> A modificação, desativação ou exclusão de rotas personalizadas altera o fluxo de tráfego da conexão e pode interromper qualquer sessão de usuário que possa estar ativa.

Para adicionar uma rota personalizada:

1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita.
2. Selecione a conexão que você deseja excluir.
3. Nos detalhes da conexão, selecione **Routes** e, em seguida, selecione **Add Route**.
4. Insira um nome amigável, o endereço IP de destino e o prefixo e o tipo de salto seguinte que você deseja usar. Se você selecionar **Virtual Appliance** como o tipo de salto seguinte, digite o endereço IP interno do equipamento.
5. Indique se você deseja ativar a rota personalizada. Por padrão, a rota personalizada está habilitada.

6. Selecione **Add Route**.

Para modificar ou desativar uma rota personalizada:

1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita.
2. Selecione a conexão que você deseja excluir.
3. Nos detalhes da conexão, selecione **Routes** e localize a rota personalizada que você deseja gerenciar.
4. No menu de reticências, selecione **Edit**.



5. Faça as alterações necessárias no endereço IP e prefixo de destino ou no tipo de próximo salto, conforme necessário.
6. Para ativar ou desativar uma rota personalizada, em **Enable this route?**, selecione **Yes** ou **No**.
7. Selecione **Save**.

Para excluir uma rota personalizada:

1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita.
2. Selecione a conexão que você deseja excluir.
3. Nos detalhes da conexão, selecione **Routes** e localize a rota personalizada que você deseja gerenciar.
4. No menu de reticências, selecione **Delete**.
5. Selecione **eleting a route may disrupt active sessions** para reconhecer o impacto da exclusão da rota personalizada.
6. Selecione **Delete Route**.

Excluir uma conexão emparelhada do Azure VNet

Antes de excluir uma conexão emparelhada do Azure VNet, remova todos os catálogos associados a ela. Consulte Delete a catalog.

1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita.
2. Selecione a conexão que você deseja excluir.
3. Nos detalhes da conexão, selecione **Delete Connection**.

Sobre as conexões SD-WAN

O Citrix SD-WAN otimiza todas as conexões de rede necessárias para o Citrix DaaS. Trabalhando em conjunto com as tecnologias HDX, o Citrix SD-WAN fornece qualidade de serviço e confiabilidade de conexão para o tráfego ICA e Citrix DaaS fora de banda. O Citrix SD-WAN suporta as seguintes conexões de rede:

- Conexão ICA multi-stream entre usuários e seus desktops virtuais
- Acesso à Internet da área de trabalho virtual para sites, aplicativos SaaS e outras propriedades de nuvem
- Acesso da área de trabalho virtual de volta aos recursos locais, como Active Directory, servidores de arquivos e servidores de banco de dados
- Tráfego interativo/em tempo real transportado pelo RTP do mecanismo de mídia no aplicativo Workspace para serviços de Unified Communications hospedados na nuvem, como o Microsoft Teams
- Busca do lado do cliente de vídeos de sites como YouTube e Vimeo

Conforme mostrado no gráfico a seguir, você cria uma conexão SD-WAN a partir da assinatura do Citrix Managed Azure para seus sites. Durante a criação da conexão, os dispositivos SD-WAN VPX são criados na assinatura do Citrix Managed Azure. Do ponto de vista da SD-WAN, esse local é tratado como uma ramificação.



Requisitos e preparação da conexão SD-WAN

- Se os seguintes requisitos não forem atendidos, a opção de conexão de rede SD-WAN não estará disponível.
    - Direitos do serviço Citrix Cloud: Citrix DaaS (antigo serviço Citrix Virtual Apps and Desktops) e SD-WAN Orchestrator.
    - Uma implantação de SD-WAN instalada e configurada. A implantação deve incluir um Master Control Node (MCN), seja na nuvem ou no local, e ser gerenciada com o SD-WAN Orchestrator.
- Intervalo de IP da VNet: forneça um espaço de endereço CIDR disponível (endereço IP e prefixo de rede) exclusivo entre os recursos de rede que estão sendo conectados. Esse é o intervalo de IP atribuído às VMs na VNet do Citrix DaaS.

Tenha o cuidado de especificar um intervalo de IP que não se sobreponha a nenhum endereço usado na nuvem e nas redes locais.

- Por exemplo, se sua rede tiver um espaço de endereço de 10.0.0.0 /16, crie a conexão no Citrix DaaS como algo como 192.168.0.0 /24.
- Neste exemplo, criar uma conexão com um intervalo de IP 10.0.0.0 /24 seria considerado um intervalo de endereços sobreposto.

Se os endereços se sobrepuserem, poderá não ser possível criar a conexão. Também não funciona corretamente para tarefas de administração do site.

- O processo de configuração da conexão inclui tarefas que você (administrador do Citrix DaaS) e o administrador do SD-WAN Orchestrator devem concluir. Além disso, para concluir suas tarefas, você precisa de informações fornecidas pelo administrador do SD-WAN Orchestrator.

  Recomendamos que você revise a orientação neste documento, além da documentação da SD-WAN, antes de criar uma conexão de fato.

Criar uma conexão SD-WAN

> **Importante:**
>
> Para obter detalhes sobre a configuração de SD-WAN, consulte SD-WAN configuration for Citrix DaaS integration.

1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita.
2. Selecione **Add Connection**.
3. Na página **Add a network connection**, clique em qualquer lugar na caixa SD-WAN.
4. A próxima página resume o que vem em seguida. Quando terminar de ler, selecione **Start Configuring SD-WAN**.
5. Na página **Configure SD-WAN**, insira as informações fornecidas pelo administrador do SD-WAN Orchestrator.

   - **Deployment mode:** se você selecionar **High availability**, dois dispositivos VPX serão criados (recomendado para ambientes de produção). Se você selecionar **Standalone**, será criado um equipamento. Você não pode alterar essa configuração posteriormente. Para mudar para o modo de implantação, você terá que excluir e recriar o branch e todos os catálogos associados.

- **Name:** digite um nome para o site da SD-WAN.
- **Throughput and number of offices:** essas informações são fornecidas pelo administrador do SD-WAN Orchestrator.
- **Region:** a região onde os dispositivos VPX serão criados.
- **VDA subnet and SD-WAN subnet:** essas informações são fornecidas pelo administrador do SD-WAN Orchestrator. Consulte SD-WAN connection requirements and preparation para obter informações sobre como evitar conflitos.

6. Quando terminar, selecione **Create Branch**.
7. A próxima página resume o que procurar no painel **Manage > Quick Deploy** \. Quando terminar de ler, selecione **Got it**.
8. Em **Manage > Quick Deploy**, a nova entrada SD-WAN em **Network Connections** mostra o andamento do processo de configuração. Quando a entrada ficar laranja com a mensagem `Awaiting activation by SD-WAN administrator`, notifique o administrador do SD-WAN Orchestrator.
9. Para tarefas de administrador do SD-WAN Orchestrator, consulte a documentação do produto SD-WAN Orchestrator.
10. Quando o administrador do SD-WAN Orchestrator terminar, a entrada SD-WAN em **Network Connections** passará para a cor verde, com a mensagem `You can create catalogs using this connection`.

Exibir detalhes da conexão SD-WAN

1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita.
2. Selecione **SD-WAN** se essa não for a única seleção.
3. Selecione a conexão que você deseja exibir.

A tela inclui:

- **Details tab:** Informações que você especificou ao configurar a conexão.
- **Branch Connectivity tab:** nome, conectividade de nuvem, disponibilidade, camada de largura de banda, função e local para cada filial e MCN.

Excluir uma conexão SD-WAN

Antes de excluir uma conexão SD-WAN, remova todos os catálogos associados a ela. Consulte Delete a catalog.

1. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita.
2. Selecione SD-WAN se essa não for a única seleção.
3. Selecione a conexão que você deseja excluir para expandir seus detalhes.
4. Na guia **Details**, selecione **Delete Connection**.
5. Confirme a exclusão.

Referência ao Quick Deploy

Guias do catálogo no painel do Quick Deploy

No painel **Manage > Quick Deploy** no Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), clique em qualquer lugar na entrada do catálogo. As guias a seguir contêm informações sobre o catálogo:

- **Details:** lista as informações especificadas quando o catálogo foi criado (ou sua edição mais recente). Também contém informações sobre a imagem que foi usada para criar o catálogo.

  Nessa guia, você pode:

  - Alterar a imagem usada no catálogo.
  - Excluir o catálogo.
  - Acessar a página que contém detalhes do local do recurso usado pelo catálogo.

- **Desktop:** disponível somente para catálogos contendo máquinas de sessão única (estáticas ou aleatórias). Nessa guia, você pode alterar o nome e a descrição do catálogo.
- **Desktop and Apps:** a guia **Desktop and Apps** está disponível somente para catálogos contendo máquinas multissessão. Nessa guia, você pode:

  - Adicionar, editar ou remover aplicativos que os usuários do catálogo possam acessar no Citrix Workspace.
  - Alterar o nome e a descrição do catálogo.

- **Subscribers:** lista todos os usuários, incluindo o tipo (usuário ou grupo), nome da conta, nome de exibição, além do domínio do Active Directory e do nome UPN.

  Nessa guia, você pode adicionar ou remover usuários de um catálogo.

- **Machines:** mostra o número total de máquinas no catálogo, além do número de máquinas registradas, máquinas não registradas e máquinas que têm o modo de manutenção ativado.

Para cada máquina no catálogo, a exibição inclui o nome de cada máquina, estado de energia (ligado/desligado), estado de registro (registrado/não registrado), usuários atribuídos, contagem de sessões (0/1) e status do modo de manutenção (um ícone indicando ligado ou desligado).

Nessa guia, você pode:

- Adicionar ou excluir uma máquina
- Iniciar, reinicializar, forçar a reinicialização ou desligar uma máquina
- Ativar ou desativar o modo de manutenção de uma máquina

Para obter detalhes, consulte Gerenciar catálogos. Muitas das ações da máquina também estão disponíveis na guia **Monitor** no painel Quick Deploy. Consulte Monitorar e controlar a energia das máquinas.

- **Power Management:** permite gerenciar quando as máquinas no catálogo são ligadas e desligadas. Uma programação também indica quando as máquinas ociosas são desconectadas.

  Você pode configurar uma programação de energia quando cria um catálogo personalizado ou posteriormente. Se não houver uma programação agendada explicitamente, uma máquina será desligada quando uma sessão terminar.

  Quando cria um catálogo usando o modo de criação rápida, você não pode selecionar ou configurar uma programação de energia. Por padrão, os catálogos de criação rápida usam a programação predefinida de Cost Saver. No entanto, você pode editar o catálogo posteriormente e alterar a programação.

  Para obter detalhes, consulte Gerenciar programações de gerenciamento de energia.

Servidores DNS

Esta seção se aplica a todas as implantações que contêm máquinas ingressadas no domínio. Você pode ignorar esta seção se usar somente máquinas não ingressadas no domínio.

1. Antes de criar um catálogo ingressado no domínio (ou uma conexão, se estiver usando uma assinatura do Citrix Managed Azure), verifique se você tem entradas de servidor DNS que podem resolver nomes de domínios públicos e privados.

   Quando o Citrix DaaS cria um catálogo ou uma conexão, ele procura por pelo menos uma entrada de servidor DNS válida. Se nenhuma entrada válida for encontrada, a operação de criação falhará.

Onde verificar:

- Se você estiver usando sua própria assinatura do Azure, verifique as entradas de **servidores DNS** no seu Azure.
- Se você estiver usando uma assinatura do Citrix Managed Azure e criando uma conexão de emparelhamento da VNet do Azure, verifique as entradas de **servidores DNS** na VNet do Azure que está emparelhando.
- Se você estiver usando uma assinatura do Citrix Managed Azure e criando uma conexão SD-WAN, verifique as entradas DNS no SD-WAN Orchestrator.

2. No Azure, a configuração **Custom** deve ter pelo menos uma entrada válida. Esse serviço não pode ser usado com a configuração **Default (Azure-provided)**.

   - Se **Default (Azure-provided)** estiver habilitado, altere a configuração para **Custom** e adicione pelo menos uma entrada de servidor DNS.
   - Se você já tiver entradas de servidores DNS em **Custom**, verifique se as entradas que deseja usar com o serviço podem resolver nomes de IP de domínio público e privado.
   - Se você não tiver nenhum servidor DNS que possa resolver nomes de domínio, a Citrix recomenda adicionar um servidor DNS fornecido pelo Azure que tenha o recurso.

3. Se você alterar qualquer entrada do servidor DNS, reinicie todas as máquinas conectadas à rede virtual. A reinicialização atribui as novas configurações do servidor DNS. (As máquinas virtuais continuam usando suas configurações de DNS atuais até a reinicialização.)

   Se você quiser alterar os endereços DNS posteriormente, depois que uma conexão for criada:

- Quando usar sua própria assinatura do Azure, você pode alterá-los no Azure (conforme descrito nas etapas anteriores). Ou você pode alterá-los no serviço.
- Quando usar uma assinatura do Citrix Managed Azure, esse serviço não sincroniza as alterações ao endereço de DNS que você faz no Azure. No entanto, você pode alterar as configurações de DNS da conexão do serviço.

Lembre-se de que a alteração de endereços de servidor DNS pode causar problemas de conectividade para máquinas em catálogos que usam essa conexão.

Adicionar servidores DNS por meio do serviço

Antes de adicionar um endereço de servidor DNS a uma conexão, confirme que o servidor DNS pode resolver nomes de domínios públicos e internos. A Citrix recomenda que você teste a conectividade ao servidor DNS antes de adicioná-lo.

1. Para adicionar, alterar ou remover um endereço de servidor DNS ao criar uma conexão, selecione **Edit DNS servers** na página **Add** *connection type*. Ou, se uma mensagem indicar que nenhum endereço de servidor DNS foi encontrado, selecione **Add DNS Servers**. Vá para a etapa 3.
2. Para adicionar, alterar ou remover um endereço de servidor DNS de uma conexão existente:
    a. Em **Manage > Quick Deploy**, expanda **Network Connections** à direita.
    b. Selecione a conexão que deseja editar.
    c. Selecione **Edit DNS servers**.
3. Adicione, altere ou remova endereços.
    a. Para adicionar um endereço, selecione **Add DNS server** e digite o endereço IP.
    b. Para alterar um endereço, clique dentro do campo de endereço e altere os números.
    c. Para remover um endereço, selecione o ícone de lixeira ao lado da entrada de endereço. Você não pode remover todos os endereços de servidor DNS. A conexão deve ter pelo menos um.
4. Quando terminar, selecione **Confirm Changes** na parte inferior da página.
5. Reinicie todas as máquinas que usam essa conexão. A reinicialização atribui as novas configurações do servidor DNS. (As máquinas virtuais continuam usando suas configurações de DNS atuais até a reinicialização.)

Políticas

Definir políticas de grupo para máquinas não ingressadas no domínio

1. Usando o protocolo RDP, conecte-se à máquina que está sendo usada para a imagem.
2. Instale o Gerenciamento de política de grupo Citrix:
    a. Navegue para CTX220345. Baixe o anexo.

   b. Clique duas vezes no arquivo baixado. Na pasta `Group Policy Templates 1912 > Group Policy Management`, clique duas vezes em `CitrixGroupPolicyManagement_x64.msi`.

3. Usando o comando **Executar**, inicie `gpedit.msc` para abrir o Editor de Política de Grupo.
4. Em `User Configuration Citrix Policies > Unfiltered`, selecione **Edit Policy**.

   Se o Console de gerenciamento de política de grupo falhar (conforme descrito em CTX225742), instale o Microsoft Visual C++ 2015 Runtime (ou uma versão posterior do Runtime).
5. Ative as configurações de política conforme necessário. Por exemplo:

   - Quando trabalhar em **Computer Configuration** ou **User Configuration** (dependendo do que deseja configurar) na guia **Settings**, em `Category > ICA / Printing`, selecione **Auto-create PDF Universal Printer** e defina como `Enabled`.
   - Se quiser que os usuários conectados sejam administradores da área de trabalho, adicione o grupo **Interactive User** ao grupo interno de administradores.
6. Quando terminar, salve a imagem.
7. Atualize o catálogo existente ou crie um novo catálogo usando a nova imagem.

Definir políticas de grupo para máquinas ingressadas no domínio

1. Confirme que o recurso de Gerenciamento de política de grupo está instalado.

   - Em uma máquina multissessão Windows, adicione o recurso Gerenciamento de política de grupo usando a ferramenta do Windows para adicionar funções e recursos (como **Adicionar funções e recursos**).
   - Em uma máquina de sessão única Windows, instale as Ferramentas de Administração do Servidor Remoto para o SO apropriado. (Essa instalação requer uma conta de administrador de domínio.) Após a instalação, o Console de gerenciamento de política de grupo estará disponível no menu **Iniciar**.
2. Baixe e instale o pacote de gerenciamento da Política de Grupo Citrix na página de download da Citrix e, em seguida, defina as configurações da política conforme necessário. Siga o procedimento em Definir políticas de grupo para máquinas não ingressadas no domínio da etapa 2 até o final.

Consulte os artigos de referência de configurações de política para saber o que está disponível. Todos os recursos de política estão disponíveis na interface Full Configuration do Citrix DaaS.

Ações nos locais de recursos

A Citrix cria automaticamente um local de recursos e dois Cloud Connectors quando você cria o primeiro catálogo para publicar áreas de trabalho e aplicativos. Você pode especificar algumas informações relacionadas ao local de recursos quando criar um catálogo. Consulte Configurações de localização de recursos ao criar um catálogo.

Para o acesso ao PC remoto, você cria o local de recursos e os Cloud Connectors.

Esta seção descreve as ações disponíveis depois que um local de recursos é criado.

1. Em **Manage > Quick Deploy**, expanda **Subscriptions** à direita.
2. Selecione a assinatura.

    - A guia **Details** mostra o número e os nomes de catálogos e imagens na assinatura. Também indica o número de máquinas que podem fornecer áreas de trabalho ou aplicativos. Essa contagem não inclui máquinas usadas para outros fins, como imagens, Cloud Connectors ou servidores de licenças RDS.
    - A guia **Resource Locations** lista cada local de recursos. Cada entrada de local de recursos inclui o status e o endereço de cada Cloud Connector no local de recursos.

O menu de reticências na entrada de um local de recursos contém as seguintes ações.

Executar verificação de integridade, em Run Health Check

Selecionar **Run Health Check** inicia a verificação de conectividade imediatamente. Se a verificação falhar, o estado do Cloud Connector será desconhecido, porque ele não está se comunicando com o Citrix Cloud. Reinicie o Cloud Connector.

Reinicializar conectores, em Restart Connectors

A Citrix recomenda reiniciar apenas um Cloud Connector por vez. A reinicialização deixa o Cloud Connector offline e interrompe o acesso do usuário e a conectividade da máquina.

Marque a caixa de seleção do Cloud Connector que deseja reinicializar. Selecione **Restart**.

Adicionar conectores, em Add Connectors

A adição de um Cloud Connector normalmente leva 20 minutos para ser concluída.

Forneça as seguintes informações:

- Quantos Cloud Connectors adicionar.

- Credenciais da conta de serviço de domínio, que são usadas para ingressar as máquinas do Cloud Connector no domínio.
- Desempenho da máquina.
- Grupo de recursos do Azure. O padrão é o último grupo de recursos usado pelo local de recursos.
- Organizational Unit (OU). O padrão é a UO usada pela última vez pelo local de recursos.
- Se sua rede requer ou não um servidor proxy para conectividade com a Internet. Se você indicar que **sim**, forneça o endereço IP ou FQDN do servidor proxy e o número da porta.

Quando terminar, selecione **Add Connectors**.

Excluir conectores, em Delete Connectors

Se um Cloud Connector não conseguir se comunicar com o Citrix Cloud e uma reinicialização não resolver o problema, o suporte Citrix pode recomendar a exclusão do Cloud Connector.

Marque a caixa de seleção do Cloud Connector que deseja excluir. Em seguida, selecione **Delete**. Quando solicitado, confirme a exclusão.

Você também pode excluir um Cloud Connector disponível. No entanto, se a exclusão do Cloud Connector resultar em menos de dois Cloud Connectors disponíveis no local de recursos, você não pode excluir o Cloud Connector selecionado.

Selecionar horário de atualização, em Select Update Time

A Citrix fornece automaticamente atualizações de software para os Cloud Connectors. Durante uma atualização, um Cloud Connector é colocado offline e atualizado, enquanto outros Cloud Connectors permanecem em serviço. Quando a primeira atualização é concluída, outro Cloud Connector é colocado offline e atualizado. Esse processo continua até que todos os Cloud Connectors no local de recursos sejam atualizados. O melhor momento para iniciar as atualizações geralmente é fora do horário comercial regular.

Escolha um horário para iniciar as atualizações ou indique que você deseja que as atualizações sejam iniciadas quando uma atualização estiver disponível. Quando terminar, selecione **Save**.

Renomear, em Rename

Insira o novo nome para o local de recursos. Selecione **Save**.

Configurar conectividade, em Configure Connectivity

Indique se os usuários podem acessar áreas de trabalho e aplicativos por meio do serviço Citrix Gateway ou somente de dentro de sua rede corporativa.

Profile Management

O Profile Management garante que as configurações pessoais se apliquem aos aplicativos virtuais dos usuários, independentemente da localização do dispositivo do usuário.

A configuração do Profile Management é opcional.

Você pode ativar o Profile Management com o serviço de otimização de perfil. O serviço fornece uma maneira confiável de gerenciar essas configurações no Windows. O gerenciamento de perfis garante uma experiência consistente, mantendo um único perfil que segue o usuário. Ele consolida automaticamente e otimiza os perfis de usuário para minimizar os requisitos de gerenciamento e armazenamento. O serviço de otimização de perfil requer o mínimo em administração, suporte e infraestrutura. Além disso, a otimização de perfil fornece aos usuários uma experiência aprimorada de logon e logoff.

O serviço de otimização de perfil requer um compartilhamento de arquivos em que todas as configurações pessoais persistam. Você gerencia os servidores de arquivos. Recomendamos configurar a conectividade de rede para permitir o acesso a esses servidores de arquivos. Você deve especificar o compartilhamento de arquivos como um caminho UNC. O caminho pode conter variáveis de ambiente do sistema, atributos de usuário do Active Directory ou variáveis do Profile Management. Para saber mais sobre o formato da cadeia de texto UNC, consulte Especificar o caminho para o armazenamento do usuário.

Ao ativar o Profile Management, considere otimizar ainda mais o perfil do usuário configurando o redirecionamento de pasta para minimizar os efeitos do tamanho do perfil do usuário. A aplicação do redirecionamento de pasta complementa a solução Profile Management. Para obter mais informações, consulte Redirecionamento de pasta da Microsoft.

Configurar um servidor de licenças Microsoft RDS para cargas de trabalho do Windows Server

Este serviço acessa os recursos da sessão remota do Windows Server ao entregar uma carga de trabalho do Windows Server, como o Windows 2016. Normalmente, isso requer uma licença de acesso ao cliente dos Serviços de Área de Trabalho Remota (RDS CAL). A máquina Windows em que o Citrix VDA está instalado deve ser capaz de entrar em contato com um servidor de licenças RDS para solicitar RDS CALs.

Instale e ative o servidor de licenças. Para obter mais informações, consulte o documento Microsoft Activate the Remote Desktop Services license server Para ambientes de prova de conceito, você pode usar o período de tolerância fornecido pela Microsoft.

Com esse método, você pode fazer com que o Citrix DaaS aplique as configurações do servidor de licenças. Você pode configurar o servidor de licenças e o modo por usuário no console RDS na imagem. Você também pode configurar o servidor de licenças usando as configurações da Política de Grupo da Microsoft. Para obter mais informações, consulte o documento da Microsoft License your RDS deployment with client access licenses (CALs).

Para configurar o servidor de licenças RDS usando as configurações da política de grupo

1. Instale um Servidor de Licenças de Serviços de Área de Trabalho Remota em uma das máquinas virtuais disponíveis. A máquina virtual deve estar sempre disponível. As cargas de trabalho do Citrix DaaS devem poder alcançar esse servidor de licenças.
2. Especifique o endereço do servidor de licenças e o modo de licença por usuário usando a Política de Grupo da Microsoft. Para obter detalhes, consulte o documento da Microsoft Specify the Remote Desktop Licensing Mode for an RD Session Host Server

As cargas de trabalho do Windows 10 exigem a ativação da licença do Windows 10 apropriada. Recomendamos que você siga a documentação da Microsoft para ativar as cargas de trabalho do Windows 10.

Uso confirmado de consumo

> **Nota:**

> Esse recurso está como Preview.

> Em **Manage > Quick Deploy**, selecione o cartão **General**. O valor em **Consumption** indica qual foi o consumo usado no mês do calendário atual. Esse valor inclui compromissos mensais e com prazo.

Quando você seleciona **General**, a guia **Notifications** inclui:

- Consumo total usado para o mês (mensal e com prazo).
- Número de unidades de compromisso mensal de consumo.
- Porcentagem do compromisso de consumo com prazo.

Os valores e as barras de progresso podem alertá-lo sobre excedentes de uso potenciais ou reais.

Os dados reais podem levar 24 horas para serem exibidos. Os dados de uso e faturamento são considerados finais 72 horas após o fim de um mês.

Para obter mais informações sobre o uso, consulte Monitorar licenças e uso ativo.

Opcionalmente, você pode solicitar que as notificações apareçam no painel **Manage > Quick Deploy** quando o uso de consumo (para compromissos mensais, com prazo ou ambos) atingir um nível especificado. Por padrão, as notificações estão desativadas.

1. Na guia **Notifications**, selecione **Edit Notification Preferences**.
2. Para ativar as notificações, clique no controle deslizante para que a marca de seleção apareça.
3. Insira um valor. Repita o procedimento para o outro tipo de consumo, se necessário.
4. Selecione **Save**.

Para desativar as notificações, clique no controle deslizante para que a marca de seleção não apareça mais e selecione **Save**.

Monitorar o uso de licença Citrix

Para visualizar as informações de uso da licença Citrix, siga as orientações em Monitorar licenças e uso ativo. Você pode ver:

- Resumo do licenciamento
- Relatórios de uso
- Tendências de uso e atividade de licença
- Usuários licenciados

Você também pode liberar licenças.

Balanceamento de carga

O balanceamento de carga se aplica a máquinas multissessão, não a máquinas de sessão única.

> **Importante:**

> Alterar o método de balanceamento de carga afeta todos os catálogos em sua implantação. Isso inclui todos os catálogos criados usando qualquer tipo de host compatível, baseado em

> nuvem e no local, independentemente da interface usada para criá-los (seja Full Configuration ou Quick Deploy).

> Confirme que você tem limites máximos de sessão configurados para todos os catálogos antes de continuar.

> - Em Quick Deploy, a configuração está localizada na guia **Details** de cada catálogo.
> - Em Full Configuration, consulte Balancear a carga das máquinas.

> O balanceamento de carga mede a carga da máquina e determina qual máquina multissessão selecionar para uma sessão de usuário de entrada nas condições atuais. Essa seleção é baseada no método de balanceamento de carga configurado.

Você pode configurar um dos dois métodos de balanceamento de carga: horizontal ou vertical. O método se aplica a todos os catálogos multissessão (e, portanto, a todas as máquinas multissessão) em sua implantação do Citrix DaaS.

- **Balanceamento de carga horizontal:** uma sessão de usuário de entrada é atribuída à máquina ligada com menos carga e disponível.

  Exemplo simples: você tem duas máquinas configuradas para 10 sessões cada. A primeira máquina lida com cinco sessões simultâneas. A segunda máquina lida com cinco.

  O balanceamento de carga horizontal oferece alto desempenho ao usuário, mas pode aumentar os custos à medida que mais máquinas são mantidas ligadas e ocupadas.

  Esse método está ativado por padrão.

- **Balanceamento de carga vertical:** uma sessão de usuário de entrada é atribuída à máquina ligada com o índice de carga mais alto. O Citrix DaaS calcula e atribui um índice de carga para cada máquina multissessão. O cálculo considera fatores como CPU, memória e simultaneidade.

  Esse método satura as máquinas existentes antes de passar para as novas máquinas. À medida que os usuários se desconectam e liberam capacidade nas máquinas existentes, uma nova carga é atribuída a elas.

Exemplo simples: você tem duas máquinas configuradas para 10 sessões cada. A primeira máquina lida com as 10 primeiras sessões simultâneas. A segunda máquina lida com a décima primeira sessão.

Com o balanceamento de carga vertical, as sessões maximizam a capacidade da máquina ligada, o que pode economizar custos com a máquina.

Para configurar o método de balanceamento de carga:

1. Em **Manage > Quick Deploy**, expanda **General** à direita.
2. Em **Global Settings**, selecione **View All**.
3. Na página **Global Settings**, em **Multi-Session Catalog Load Balancing**, escolha o método de balanceamento de carga.
4. Selecione **Confirmar**.

Criar um catálogo em uma rede que usa um servidor proxy

Siga este procedimento se a sua rede exigir um servidor proxy para conectividade com a Internet e você estiver usando sua própria assinatura do Azure. (O uso de uma assinatura do Citrix Managed Azure com uma rede que exige um servidor proxy não é suportado.)

1. Em **Manage > Quick Deploy**, inicie o processo de criação do catálogo fornecendo as informações necessárias e selecionando **Create Catalog** na parte inferior da página.
2. A criação do catálogo falha devido ao requisito de proxy. No entanto, um local de recursos é criado. O nome desse local de recursos começa com “DAS”, a menos que você tenha fornecido um nome de local de recursos ao criar o catálogo. No painel **Manage > Quick Deploy**, expanda **Cloud Subscriptions** à direita. Na guia **Resource Locations**, verifique se o local de recursos recém-criado tem Cloud Connectors nele. Se tiver, exclua-os.
3. No Azure, crie duas máquinas virtuais (consulte Requisitos de sistema do Cloud Connector). Ingresse essas máquinas no domínio.
4. No console do Citrix Cloud, instale um Cloud Connector em cada máquina virtual. Verifique se os Cloud Connectors estão no mesmo local de recursos que foi criado anteriormente. Siga as orientações em:

    - Configuração de proxy e firewall do Cloud Connector
    - Requisitos de sistema e conectividade

5. Em **Manage > Quick Deploy**, repita o processo de criação do catálogo. Quando o catálogo é criado, ele usa o local de recursos e os Cloud Connectors que você criou nas etapas anteriores.

Obtenha ajuda

- Veja a Solução de problemas.
- Se precisar de mais assistência com o Citrix DaaS, abra um tíquete seguindo as orientações em Como obter ajuda e suporte.

Acesso remoto ao PC no Quick Deploy

Introdução

O Citrix Remote PC Access permite que os usuários usem remotamente máquinas físicas Windows ou Linux localizadas no escritório. Os usuários têm uma melhor experiência de usuário quando usam o Citrix HDX para entregar suas sessões do PC do escritório.

O Remote PC Access é compatível com máquinas ingressadas no domínio.

Este artigo descreve como criar uma implantação de acesso ao PC remoto usando a interface do Quick Deploy. Para criar uma implantação de acesso ao PC remoto usando a interface Full Configuration, consulte Remote PC Access.

Diferenças entre fornecer áreas de trabalho e aplicativos virtuais

Se você estiver familiarizado com o fornecimento de áreas de trabalho e aplicativos virtuais, o recurso Remote PC Access tem várias diferenças:

- Um catálogo de acesso ao PC remoto geralmente contém máquinas físicas existentes. Portanto, você não precisa preparar uma imagem ou provisionar máquinas para usar o Remote PC Access. A entrega de áreas de trabalho e aplicativos geralmente usa máquinas virtuais (VMs), e uma imagem é usada como modelo para provisionar as VMs.
- Quando uma máquina em um catálogo aleatório de acesso ao PC remoto é desligada, ela não é redefinida para o estado original da imagem.
- Para catálogos estáticos de atribuição de usuário do Remote PC Access, a atribuição ocorre depois que um usuário faz login (na máquina ou via RDP). Ao fornecer áreas de trabalho e aplicativos, um usuário é atribuído se uma máquina estiver disponível.

Resumo da instalação e configuração

Leia esta seção antes de iniciar as tarefas.

1. Antes de começar:
    a. Leia os Requisitos e considerações.
    b. Conclua as tarefas de preparação.
2. No Citrix Cloud:
    a. Configure uma conta do Citrix Cloud e registre-se no Citrix DaaS.
    b. Configure um local de recursos que possa acessar seus recursos do Active Directory. Instale pelo menos dois Cloud Connectors no local de recursos. Os Cloud Connectors se comunicam com o Citrix Cloud.

       Siga as orientações para criar um local de recursos e instalar Cloud Connectors nele. As informações incluem requisitos do sistema, preparação e procedimentos.
    c. Conecte seu Active Directory ao Citrix Cloud.
3. Instale um Citrix Virtual Delivery Agent (VDA) em cada máquina que os usuários acessarão remotamente. Os VDAs se comunicam com o Citrix Cloud por meio dos Cloud Connectors no local de recursos.
4. Em **Manage > Quick Deploy**:
    a. Crie um catálogo de acesso ao PC remoto. Nesse procedimento, você especifica a localização do seu local de recursos e seleciona o método de atribuição de usuário.
    b. Adicione assinantes (usuários) ao catálogo, se necessário. Adicione usuários a um catálogo se o catálogo usar o método de atribuição de usuário estático atribuído automaticamente ou aleatório de um pool. Você não precisa adicionar usuários a um catálogo estático pré-atribuído.
5. Envie o URL do espaço de trabalho para os usuários. No espaço de trabalho, os usuários podem fazer logon em suas máquinas no escritório.

Requisitos e considerações

As referências a máquinas nesta seção referem-se às máquinas que os usuários acessam remotamente.

Geral

- As máquinas devem estar executando um sistema operacional Windows 10 ou Linux (Red Hat Enterprise Linux e Ubuntu) de sessão única.
- A máquina deve ser ingressada em um domínio do Active Directory Domain Services.
- Se você estiver familiarizado com o uso do Remote PC Access com o Citrix Virtual Apps and Desktops, o recurso Wake-on-LAN não está disponível no Citrix DaaS.

Rede

- A máquina deve ter uma conexão de rede ativa. Uma conexão com fio é recomendada para ter-se maior confiabilidade e largura de banda.
- Se estiver usando Wi-Fi:
  - Defina as configurações de energia para deixar o adaptador sem fio ligado.
  - Configure o adaptador sem fio e o perfil de rede para permitir a conexão automática à rede sem fio antes que o usuário faça logon. Caso contrário, o VDA não se registra até que o usuário faça logon. A máquina não fica disponível para acesso remoto até que um usuário faça logon.
  - Certifique-se de que os Cloud Connectors possam ser acessados pela rede Wi-Fi.

Dispositivos e periféricos

- Os seguintes dispositivos não são compatíveis:
  - Chaveadores KVM ou outros componentes que podem desconectar uma sessão.
  - PCs híbridos, incluindo notebooks e PCs All-in-One e NVIDIA Optimus.
- Conecte o teclado e o mouse diretamente à máquina. Esses periféricos poderão se tornar indisponíveis se forem conectados ao monitor ou a outros componentes que podem ser desligados ou desconectados. Se você precisar conectar os dispositivos de entrada a componentes como monitores, não desative os componentes.
- Para laptops e dispositivos Surface Pro: certifique-se de que o laptop está conectado a uma fonte de alimentação em vez de estar funcionando na bateria. Configure as opções de energia do laptop para corresponder às opções de uma máquina desktop. Por exemplo:
  - Desative o recurso de hibernação.
  - Desative o recurso de suspensão.
  - Defina a ação de fechar a tampa como **Não fazer nada**.

- Defina a ação **pressionar o botão de energia** como **Desligar**.
- Desative os recursos de economia de energia da placa de vídeo e da NIC.

Quando estiver usando uma base de encaixe, você pode desencaixar e reencaixar os laptops. Quando você desencaixa o laptop, o VDA se registra novamente nos Cloud Connectors por Wi-Fi. No entanto, quando você reencaixa o laptop, o VDA não muda para a conexão com fio, a menos que você desconecte o adaptador de conexão sem fio. Alguns dispositivos fornecem funcionalidade interna para desconectar o adaptador de conexão sem fio ao estabelecer uma conexão com fio. Outros dispositivos exigem soluções personalizadas ou utilitários de terceiros para desconectar o adaptador de conexão sem fio. Revise as considerações de Wi-Fi mencionadas anteriormente.

Para ativar o encaixe e desencaixe de dispositivos Remote PC Access:

- Em **Iniciar > Configurações > Sistema > Energia e suspensão**, defina **Suspender** como **Nunca**.
- Em **Gerenciador de dispositivos > Adaptadores de rede > Adaptador Ethernet** vá para **Gerenciamento de energia** e desmarque **O computador pode desligar o dispositivo para economizar energia**. Assegure que **Permitir que este dispositivo acorde o computador** esteja selecionado.

Linux VDA

- Use o Linux VDA em máquinas físicas somente no modo não 3D. Devido a limitações do driver do NVIDIA, a tela local do PC não pode ser desligada e exibe as atividades da sessão quando o modo HDX 3D está ativado. Mostrar essa tela é um risco de segurança.
- Catálogos com máquinas Linux devem usar o método de atribuição de usuário estático pré-atribuído. Catálogos com máquinas Linux não podem usar os métodos de atribuição estático atribuído automaticamente ou aleatório de um pool.

Considerações sobre o Workspace

- Vários usuários com acesso ao mesmo PC de escritório veem o mesmo ícone no Citrix Workspace. Quando um usuário faz login no Citrix Workspace, a máquina aparece como indisponível se já estiver em uso por outro usuário.

Preparar

- Decida como instalar o VDA nas máquinas. Há vários métodos disponíveis:
  - Manualmente, instale o VDA em cada máquina.

    - Envie a instalação do VDA usando a Política de grupo, usando um script.
    - Envie a instalação do VDA usando uma ferramenta de Distribuição Eletrônica de Software (ESD), como o Microsoft System Center Configuration Manager (SCCM). Para obter detalhes, consulte Instalar VDAs usando SCCM.

- Saiba mais sobre os métodos de atribuição de usuário e decida qual método você usará. Você especifica o método ao criar um catálogo do Remote PC Access.
- Decida como as máquinas (na verdade, os VDAs que você instala nas máquinas) serão registradas no Citrix Cloud. Um VDA deve se registrar para estabelecer comunicação com o agente de sessão no Citrix Cloud.

  Os VDAs se registram por meio dos Cloud Connectors em seus locais de recursos. Você pode especificar endereços de Cloud Connectors ao instalar um VDA ou posteriormente.

  Para o primeiro registro (inicial) de um VDA, a Citrix recomenda o uso de LGPO ou GPO baseado em políticas. Após o registro inicial, a Citrix recomenda o uso da atualização automática, que é ativada por padrão. Saiba mais sobre o registro do VDA.

Instale um VDA

Baixe e instale um VDA em cada máquina física que os usuários acessarão remotamente.

Download de um VDA

- Para baixar um Windows VDA:

  a. Usando suas credenciais de conta do Citrix Cloud, navegue até a página de download do Citrix DaaS.

  b. Baixe o VDA mais recente. Há dois tipos de pacotes de instalação disponíveis. Os valores de ano e mês no título do VDA variam.

- Para baixar um Linux VDA para acesso ao PC remoto, siga as orientações na documentação do Linux VDA.

Tipos de pacotes de instalação do Windows VDA

O site de download da Citrix fornece dois tipos de pacotes de instalação do Windows VDA que podem ser usados para máquinas no Remote PC Access:

- Instalador de VDA básico de sessão única (a *versão* é *aamm*):
  `VDAWorkstationCoreSetup_release.exe`

O instalador de VDA básico de sessão única é adaptado especificamente para o Remote PC Access. Ele é leve e mais fácil de implantar (do que outros instaladores de VDA) pela rede em todas as máquinas. Ele não inclui componentes que normalmente não são necessários nessas implantações, como o Citrix Profile Management, o Machine Identity Service e a camada de personalização do usuário.

No entanto, sem o Citrix Profile Management instalado, os displays do Citrix Analytics for Performance e alguns detalhes do Monitor não estarão disponíveis. Para obter detalhes sobre essas limitações, consulte a publicação do blog Monitorar e solucionar problemas em máquinas no Remote PC Access.

Se você quiser exibições completas de análise e monitoramento, use o instalador de VDA completo de sessão única.

- Instalador de VDA completo de sessão única (a *versão* é *aamm*): `VDAWorkstationSetup_release.exe`

  Embora o instalador de VDA completo de sessão única seja um pacote maior do que o instalador de VDA básico de sessão única, você pode adaptá-lo para instalar apenas os componentes necessários. Por exemplo, você pode instalar os componentes que oferecem suporte ao Profile Management.

Instalar um Windows VDA para acesso ao PC remoto de forma interativa

1. Clique duas vezes no arquivo de instalação do VDA que você baixou.
2. Na página **Environment**, selecione **Enable Remote PC Access** e clique em **Next**.
3. Na página **Delivery Controller**, selecione uma das seguintes opções:

   - Se você souber o endereço dos seus Cloud Connectors, selecione **Do it manually**. Insira o FQDN de um Cloud Connector e clique em **Add**. Repita o procedimento para os outros Cloud Connectors no seu local de recursos.
   - Se você souber onde instalou os Cloud Connectors na sua estrutura do AD, selecione **Choose locations from Active Directory** e navegue até o local. Repita o procedimento para os outros Cloud Connectors.
   - Se você quiser especificar o endereço dos Cloud Connectors na Política de Grupo Citrix, selecione **Do it later (Advanced)** e confirme a seleção quando solicitado.

   Quando terminar, clique em **Next**.
4. Se você estiver usando o instalador VDA completo de sessão única, na página **Additional Components**, selecione os componentes que deseja instalar, como o Profile Management.

(Essa página não aparece se você estiver usando o instalador de VDA básico de sessão única.)

5. Na página **Features**, clique em **Next**.
6. Na página **Firewall**, selecione **Automatically** (se ainda não estiver). Clique em **Next**.
7. Na página **Summary**, clique em **Install**.
8. Na página **Diagnose**, clique em **Connect**. Confirme que a caixa de seleção esteja marcada. Quando solicitado, insira as credenciais da sua conta da Citrix. Depois que suas credenciais forem validadas, clique em **Next**.
9. Na página **Finish**, clique em **Finish**.

Para obter informações completas sobre a instalação, consulte Instalar VDAs.

Instalar um Windows VDA para acesso ao PC remoto usando uma linha de comando

- Se você estiver usando o instalador de VDA básico de sessão única: execute `VDAWorkstationCoreSetup.exe` e inclua as opções `/quiet`, `/enable_hdx_ports` e `/enable_hdx_udp_ports`. Para especificar endereços do Cloud Connector, use a opção `/controllers`.

  Por exemplo, o comando a seguir instala um VDA básico de sessão única. O aplicativo Citrix Workspace e outros serviços não principais não são instalados. O FQDN dos dois Cloud Connectors é especificado e as portas no Serviço do Firewall do Windows serão abertas automaticamente. O administrador lidará com as reinicializações.

  ```
  VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East.domain.com" “Connector-East2.domain.com” /enable_hdx_ports /noreboot
  ```

- Se você estiver usando o instalador de VDA completo de sessão única e quiser incluir o Profile Management (ou outros componentes opcionais): execute `VDAWorkstationSetup.exe` e inclua as opções `/remotepc` e `/includeadditional`. A opção `/remotepc` impede a instalação da maioria dos componentes adicionais. A opção `/includeadditional` especifica exatamente quais componentes adicionais você deseja instalar.

  Por exemplo, o comando a seguir impede a instalação de todos os componentes adicionais opcionais, exceto o Profile Management.

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /includeadditional “Citrix User Profile Manager”,“Citrix User Profile Manager WMI Plugin” /controllers “connector.domain.com” “connector2.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

Para obter detalhes, consulte Opções de linha de comando para instalar um VDA.

Instalar um Linux VDA

Siga as orientações na documentação do Linux para instalar um Linux VDA interativamente ou usando a linha de comando.

Criar um catálogo de acesso ao PC remoto

Um local de recursos contendo pelo menos dois Cloud Connectors deve existir antes que você possa criar um catálogo com êxito.

> **Importante:**
>
> Uma máquina só pode pertencer a um catálogo por vez. Essa restrição não é imposta quando você especifica as máquinas a serem adicionadas a um catálogo. No entanto, ignorar a restrição pode causar problemas posteriormente.

1. Faça login no Citrix Cloud.
2. No menu superior esquerdo, selecione **My Services > DaaS**.
3. Se você ainda não criou nenhum catálogo, clique em **Get Started** na página de **boas-vindas**.
4. Selecione **Manage > Quick Deploy**.
5. Selecione **Create Catalog**.
6. Na guia **Remote PC Access**, selecione um método para atribuir usuários às máquinas.
7. Insira um nome para o catálogo e selecione o local de recursos que você criou.
8. Adicione máquinas.
9. Clique em **Create Catalog**.
10. Na página **Your Remote PC Access catalog is being created**, clique em **Done**.
11. Aparece uma entrada para o novo catálogo no painel **Manage > Quick Deploy**.

    Depois que o catálogo for criado com êxito, clique em um dos links para adicionar assinantes (usuários) ao catálogo. Esta etapa se aplica se o catálogo usar o método de atribuição de usuário estático autoatribuído ou aleatório de um pool não atribuído.

Depois de criar um catálogo e adicionar usuários (se necessário), envie a URL do espaço de trabalho para os seus usuários.

Métodos de atribuição do usuário

O método de atribuição do usuário escolhido ao criar um catálogo indica como os usuários são atribuídos às máquinas.

- **Atribuição automática estática:** a atribuição do usuário ocorre quando um usuário faz logon na máquina (sem usar o Citrix, por exemplo, pessoalmente ou por RDP), depois que um VDA é instalado na máquina. Posteriormente, se outros usuários fizerem logon nessa máquina (sem usar o Citrix), eles também serão atribuídos. Somente um usuário pode usar a máquina por vez. Essa é uma configuração típica para funcionários de escritório ou que trabalham por turnos e que compartilham um computador.

  Esse método é aceito com máquinas Windows. Ele não pode ser usado com máquinas Linux.
- **Pré-atribuído estático:** os usuários são pré-atribuídos às máquinas. (Isso geralmente é configurado fazendo o upload de um arquivo CSV contendo o mapeamento usuário-máquina.) Não há necessidade de logon do usuário para estabelecer a atribuição após a instalação do VDA. Também não há necessidade de atribuir usuários ao catálogo depois que ele é criado. Esse é o melhor para funcionários de escritório.

  Esse método é aceito com máquinas Windows e Linux.
- **Aleatório de um pool não atribuído:** os usuários são atribuídos aleatoriamente a uma máquina disponível. Somente um usuário pode usar a máquina por vez. Ideal para laboratórios de computação em escolas.

  Esse método é aceito com máquinas Windows. Ele não pode ser usado com máquinas Linux.

Métodos para adicionar máquinas a um catálogo

Lembre-se: toda máquina deve ter um VDA instalado nela.

Ao criar ou editar um catálogo, há três maneiras de adicionar máquinas a ele:

- Selecionar contas de máquina uma a uma.
- Selecionar unidades organizacionais (UO).
- Adicionar em massa usando um arquivo CSV. Há um modelo disponível do arquivo CSV para você usar.

Adicionar nomes de máquinas

Esse método adiciona contas de máquina uma a uma.

1. Selecione seu domínio.

2. Procure a conta da máquina.
3. Clique em **Add**.
4. Repita para adicionar mais máquinas.
5. Quando terminar de adicionar máquinas, clique em **Done**.

Adicionar UOs

Este método adiciona contas de máquina de acordo com a Unidade Organizacional em que elas residem. Ao selecionar UOs, escolha UOs de nível inferior para obter maior granularidade. Se a granularidade não for necessária, você pode escolher UOs de nível superior.

Por exemplo, no caso de `Bank/Officers/Tellers`, selecione `Tellers` para obter maior granularidade. Caso contrário, você pode selecionar `Officers` ou `Bank` de acordo com as exigências.

Mover ou excluir UOs depois que forem atribuídas a um catálogo Remote PC Access afeta associações de VDA e causa problemas com atribuições futuras. Certifique-se de que seu plano de alteração do AD contabilize as atualizações de atribuição de UO para catálogos.

Para adicionar UOs:

1. Selecione seu domínio.
2. Selecione as UOs que contêm as contas de máquinas que você deseja adicionar.
3. Indique na caixa de seleção se deseja incluir as subpastas incluídas em suas seleções.
4. Quando terminar de selecionar as UOs, clique em **Done**.

Adicionar em massa

1. Clique em **Download CSV Template**.
2. No modelo, adicione as informações da conta da máquina (até 100 entradas). O arquivo CSV também pode conter o nome dos usuários atribuídos a cada máquina.
3. Salve o arquivo.
4. Arraste o arquivo para a página **Add machines in bulk** ou navegue até o arquivo.
5. É exibida uma pré-visualização do conteúdo do arquivo. Se esse não for o arquivo desejado, você pode criar outro arquivo e arrastá-lo ou navegar até ele.
6. Quando terminar, clique em **Done**.

Gerenciar catálogos de acesso ao PC remoto

Para exibir ou alterar as informações de configuração de um catálogo do Remote PC Access, selecione o catálogo no painel **Manage > Quick Deploy** (clique em qualquer lugar na entrada do catálogo).

- Na guia **Details**, você pode adicionar ou remover máquinas.
- Na guia **Subscribers**, você pode adicionar ou remover usuários.
- Na guia **Machines**, você pode:
  - Adicionar ou remover máquinas: botão **Add or remove machines**.
  - Alterar atribuições do usuário: ícone de lixeira **Remove assignment**, **Edit machine assignment** no menu de reticências.
  - Ver quais máquinas estão registradas e colocar as máquinas dentro ou fora do modo de manutenção.

Solução de problemas no Quick Deploy

Introdução

Os locais de recursos contêm as máquinas que fornecem áreas de trabalho e aplicativos. Essas máquinas são criadas em catálogos, portanto, os catálogos são considerados parte do local de recursos. Cada local de recursos também contém Cloud Connectors. Os Cloud Connectors permitem que o Citrix Cloud se comunique com o local do recurso. Normalmente, a Citrix instala e atualiza os Cloud Connectors.

Opcionalmente, você pode iniciar vários Cloud Connector e ações de localização de recursos. Veja:

- Ações nos locais de recursos
- Configurações de localização de recursos ao criar um catálogo

O Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) tem ferramentas para solução de problemas e suporte que podem ajudar a resolver problemas de configuração e comunicação com as máquinas que fornecem áreas de trabalho e aplicativos (os VDAs). Por exemplo, a criação de um catálogo pode falhar ou os usuários podem não conseguir iniciar a área de trabalho ou os aplicativos.

Essa solução de problemas inclui obter acesso à sua assinatura do Citrix Managed Azure por meio de uma máquina bastion ou RDP direto. Depois de obter acesso à assinatura, você pode usar as ferramentas de suporte da Citrix para localizar e resolver problemas. Para obter detalhes, consulte:

- Solução de problemas de VDA usando um bastion ou RDP direto
- Acesso ao bastion
- Acesso direto ao RDP

Solução de problemas de VDA usando um bastion ou RDP direto

Os recursos de suporte são para pessoas com experiência na solução de problemas da Citrix. Isso inclui:

- Citrix Service Providers (CSP) e outros que tenham conhecimento técnico e experiência em solução de problemas com os produtos Citrix DaaS.
- Equipe de suporte Citrix.

Se não estiver familiarizado ou não se sentir seguro para desempenhar a solução de problemas de componentes Citrix, você pode solicitar ajuda do Suporte Citrix. Os representantes do Suporte Citrix podem solicitar que você configure um dos métodos de acesso descritos nesta seção. No entanto, os representantes da Citrix desempenham a real solução do problema, usando as ferramentas e tecnologias Citrix.

> **Importante:**
>
> Esses recursos de suporte são válidos somente para máquinas ingressadas no domínio. Se as máquinas em seus catálogos não tiverem ingressadas no domínio, você será orientado a solicitar ajuda para a solução do problema ao Suporte Citrix.

Métodos de acesso

Estes métodos de acesso são válidos somente para a assinatura do Citrix Managed Azure. Para obter mais informações, consulte Assinaturas do Azure.

Dois métodos de acesso de suporte são fornecidos.

- Acesse seus recursos por meio de uma máquina bastion na assinatura dedicada do Citrix Managed Azure do cliente. O bastion é um ponto de entrada único que permite o acesso às

máquinas na assinatura. Ele fornece uma conexão segura com esses recursos, permitindo o tráfego remoto de endereços IP em um intervalo especificado.

As etapas desse método incluem:

- Criar a máquina bastion
- Baixar um agente RDP
- Fazer RDP para a máquina bastion
- Conectar-se da máquina bastion às outras máquinas Citrix em sua assinatura

A máquina bastion é destinada ao uso de curto prazo. Esse método é destinado a problemas que envolvem a criação de catálogos ou máquinas de imagem.

- Acesso RDP direto às máquinas na assinatura dedicada do Citrix Managed Azure do cliente. Para permitir o tráfego RDP, a porta 3389 deve ser definida no grupo de segurança de rede.

  Esse método destina-se a problemas de catálogo não referentes a criação, como usuários que não conseguem iniciar suas áreas de trabalho.

Lembre-se: como alternativa a esses dois métodos de acesso, entre em contato com o Suporte Citrix para obter ajuda.

Acesso ao bastion

1. Em **Manage > Quick Deploy**, expanda **Troubleshoot & Support** à direita.
2. Clique em **View troubleshooting options**.
3. Na página **Troubleshoot**, selecione um dos dois primeiros tipos de problema e clique em **Use our troubleshooting machine**.
4. Na página **Troubleshoot with Bastion Machine**, selecione o catálogo.
   - Se as máquinas no catálogo selecionado não estiverem ingressadas no domínio, você será instruído a entrar em contato com o Suporte Citrix.
   - Se uma máquina bastion já tiver sido criada com acesso RDP à conexão de rede do catálogo selecionado, pule para a etapa 8.
5. O intervalo de acesso RDP é exibido. Se desejar restringir o acesso RDP a um intervalo menor do que o permitido pela conexão de rede, marque a caixa de seleção **Restrict RDP access to only computers in IP address range** e insira o intervalo desejado.
6. Digite o nome de usuário e senha que você usará para fazer login quando fizer RDP na máquina bastion. Requisitos de senha.

Não use caracteres Unicode no nome de usuário.

7. Clique em **Create Bastion Machine**.

   Quando a máquina bastion é criada com sucesso, o título da página muda para **Bastion — *conexão***.

   Se a criação da máquina bastion falhar (ou se falhar durante a operação), clique em **Delete** na parte inferior da página de notificação da falha. Tente criar a máquina bastion novamente.

   Você pode alterar a restrição de alcance RDP depois que a máquina bastion for criada. Clique em **Edit**. Insira o novo valor e clique na marca de seleção para salvar a alteração. (Clique no **X** para cancelar a alteração.)

8. Clique em **Download RDP File**.
9. Faça o RDP para o bastion usando as credenciais que você especificou ao criar o bastion. (O endereço da máquina bastion é incorporado ao arquivo RDP que você baixou.)
10. Conecte-se da máquina bastion às outras máquinas Citrix na assinatura. Assim, você pode coletar logs e executar diagnósticos.

As máquinas bastion são ligadas quando são criadas. Para economizar custos, as máquinas são desligadas automaticamente se permanecerem ociosas após a inicialização. As máquinas são excluídas automaticamente após várias horas.

Você pode gerenciar a energia de uma máquina bastion ou excluí-la usando os botões na parte inferior da página. Se você optar por excluir uma máquina bastion, deve confirmar que sabe que todas as sessões ativas na máquina terminarão automaticamente. Além disso, que também todos os dados e arquivos salvos na máquina serão excluídos.

Acesso direto ao RDP

1. Em **Manage > Quick Deploy**, expanda **Troubleshoot & Support** à direita.
2. Clique em **View troubleshooting options**.
3. Na página **Troubleshoot**, selecione **Other catalog issue**.
4. Na página **Troubleshoot with RDP Access**, selecione o catálogo.

   Se o RDP já tiver sido habilitado para a conexão de rede do catálogo selecionado, pule para a etapa 7.

5. O intervalo de acesso RDP é exibido. Se desejar restringir o acesso RDP a um intervalo menor do que o permitido pela conexão de rede, marque a caixa de seleção **Restrict RDP access to only computers in IP address range** e insira o intervalo desejado.

6. Clique em **Enable RDP Access.**

   Quando o acesso RDP é ativado com êxito, o título da página muda para **RDP Access — *conexão***.

   Se o acesso RDP não for habilitado com êxito, clique em **Retry Enabling RDP** na parte inferior da página de notificação da falha.

7. Conecte-se às máquinas usando suas credenciais de administrador do Active Directory. Assim, você pode coletar logs e executar diagnósticos.

Obtenha ajuda

Se você ainda tiver problemas, abra um tíquete seguindo as instruções em Como obter ajuda e suporte.

Usuários e autenticação no Quick Deploy

Métodos de autenticação do usuário

Os usuários devem se autenticar ao fazer login no Citrix Workspace para iniciar suas áreas de trabalho ou aplicativos.

O Quick Deploy suporta os seguintes métodos de autenticação do usuário:

- **Managed Azure AD:** Managed Azure AD é um Azure Active Directory (AAD) fornecido e gerenciado pela Citrix. Você não precisa fornecer sua própria estrutura do Active Directory. Basta adicionar seus usuários ao diretório.
- **Seu provedor de identidade:** você pode usar qualquer método de autenticação disponível no Citrix Cloud.

Nota:

- As implantações do Remote PC Access usam somente o Active Directory. Para obter detalhes, consulte Remote PC Access.
- Se você usa o Azure AD Domain Services: os UPNs de logon do Workspace devem conter o nome de domínio que foi especificado ao habilitar o Azure AD Domain Services. Logons não podem usar UPNs em domínios que você personaliza, mesmo que o domínio personalizado seja designado como primário.

A configuração da autenticação do usuário inclui os seguintes procedimentos:

1. Configure o método de autenticação do usuário no Citrix Cloud e Workspace Configuration.
2. Se você estiver usando o Managed Azure AD para autenticação de usuário, adicione usuários ao diretório.
3. Adicione usuários a um catálogo.

Configurar a autenticação do usuário no Citrix Cloud

Para configurar a autenticação do usuário no Citrix Cloud:

- Conecte-se ao método de autenticação do usuário que deseja usar. (No Citrix Cloud, você se "conecta" ou "desconecta" de um método de autenticação.)
- No Citrix Cloud, defina a autenticação do espaço de trabalho para usar o método conectado.

Nota:

O método de autenticação Managed Azure AD é configurado por padrão. Ou seja, ele é conectado automaticamente no Citrix Cloud, e a autenticação do Workspace é definida automaticamente para usar o Managed Azure AD for Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). Se você quiser usar esse método (e não tiver configurado um método diferente anteriormente), continue com Adicionar e excluir usuários no Managed Azure AD. Se o Managed Azure AD for desconectado, a autenticação do Workspace será transferida para o Active Directory. Se você quiser usar um método de autenticação diferente, siga as etapas abaixo.

Para alterar o método de autenticação:

1. Em **Manage > Quick Deploy**, selecione **User Access & Authentication** à direita.

2. Selecione **Manage User Access and Authentication**. Selecione a guia **Workspace**, se ainda não estiver selecionada. (A outra guia indica qual método de autenticação de usuário está configurado no momento.)

3. Siga o link **To set up authentication methods**. O link leva você ao Citrix Cloud. No menu de reticências, selecione **Connect** para o método desejado.

4. Enquanto ainda estiver no Citrix Cloud, selecione **Workspace Configuration** no menu superior esquerdo. Na guia **Authentication**, selecione o método desejado.

O que fazer a seguir:

- Se estiver usando o Managed Azure AD, adicione usuários ao diretório.
- Para todos os métodos de autenticação, adicione usuários ao catálogo.

Adicionar e excluir usuários no Managed Azure AD

Siga este procedimento somente se estiver usando o Managed Azure AD para autenticação do usuário no Citrix Workspace.

Você fornece o nome e o endereço de e-mail de seus usuários. Em seguida, a Citrix envia um convite por e-mail para cada um deles. O e-mail instrui os usuários a selecionar um link que os ingresse no Citrix Managed Azure AD.

- Se o usuário já tiver uma conta da Microsoft com o endereço de e-mail fornecido, essa conta será usada.
- Se o usuário não tiver uma conta da Microsoft com o endereço de e-mail, a Microsoft criará uma conta.

Para adicionar e convidar usuários para o Managed Azure AD:

1. Em **Manage > Quick Deploy**, expanda **User Access & Authentication** à direita. Selecione **Manage User Access and Authentication**.
2. Selecione a guia **Managed Azure AD**.
3. Selecione **Invite Users**.



4. Digite o nome e o endereço de e-mail de um usuário e selecione **Add User**.



5. Repita a etapa anterior para adicionar outros usuários.
6. Quando terminar de adicionar as informações do usuário, selecione **Invite Users** na parte inferior do cartão.

Para excluir um usuário do Managed Azure AD, selecione o ícone de lixeira ao lado do nome do usuário que deseja excluir do diretório. Confirme a exclusão.

O que fazer a seguir: Adicionar usuários ao catálogo

Adicionar ou remover usuários em um catálogo

Conclua este procedimento independentemente do método de autenticação usado.

1. Em **Manage > Quick Deploy**, se você não adicionou nenhum usuário a um catálogo, selecione **Add subscribers**.

   Para adicionar usuários a um catálogo que já tem usuários, clique em qualquer lugar na entrada do catálogo.
2. Na guia **Subscribers**, selecione **Manage Subscribers**.

   
3. Selecione um domínio. (Se você estiver usando o Managed Azure AD para autenticação de usuário, há apenas uma entrada no campo de domínio.) Em seguida, selecione um usuário.

   
4. Selecione outros usuários, conforme necessário. Quando terminar, selecione o **X** no canto superior direito.

Para remover usuários de um catálogo, siga as etapas 1 e 2. Na etapa 3, selecione o ícone de lixeira ao lado do nome que deseja excluir (em vez de selecionar um domínio e grupo/usuário). Essa ação remove o usuário do catálogo, não da origem (como o Managed Azure AD ou o seu próprio AD ou AAD).

O que fazer a seguir:

- Para um catálogo com máquinas multissessão, adicione aplicativos, se ainda não o fez.
- Para todos os catálogos, envie a URL do Citrix Workspace para os seus usuários.

Mais informações

Para obter mais informações sobre autenticação no Citrix Cloud, consulte Gerenciamento de identidade e acesso.

Migrar a configuração para o Citrix Cloud

Por que usar a Configuração Automatizada

Os administradores de TI responsáveis por ambientes grandes ou complexos geralmente consideram as migrações um processo tedioso. Frequentemente, eles acabam escrevendo suas próprias ferramentas para realizar essa tarefa com sucesso, pois ela tende a ser específica para seus casos de uso.

A Citrix quer ajudar a facilitar esse processo automatizando o processo de migração usando a ferramenta Automated Configuration. Os administradores podem testar facilmente as configurações atuais no Citrix Cloud e aproveitar os benefícios oferecidos pelo Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), mantendo seus ambientes atuais *intactos*. Também não há impacto no usuário final, pois a Configuração Automatizada funciona perfeitamente em segundo plano. Esses benefícios incluem sobrecarga administrativa reduzida quando a Citrix gerencia parte do back-end e do plano de controle, atualizações automáticas e personalizáveis de componentes do Citrix Cloud e outros.

A Citrix usa a configuração padrão do setor como código para fornecer um mecanismo para ajudar a automatizar os processos de migração. A Configuração Automatizada descobre e exporta um ou mais sites locais como uma coleção de arquivos de configuração. A configuração desses arquivos pode ser importada para o Citrix DaaS.

A Configuração Automatizada também permite que os administradores mesclem vários sites locais em um único site, o que evita conflitos de nomes. Os administradores podem controlar se a configuração local ou na nuvem controla os recursos.

A Configuração Automatizada não é apenas uma ferramenta de migração única, mas também pode automatizar sua configuração diária no Citrix Cloud. Mover a configuração do Citrix DaaS pode ser benéfico por vários motivos:

- Sincronizar seu site do teste ou do estágio para a produção
- Fazer Backup e restauração da sua configuração
- Atingir limites de recursos
- Migrar de uma região para outra

O vídeo de *2 minutos* a seguir fornece um rápido tour pela Configuração Automatizada.

<iframe src="https://www.youtube.com/embed/uyQ9o2L1DXQ" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Para obter informações adicionais sobre Configuração Automatizada, consulte Proof of Concept: Automated Configuration Tool na Tech Zone.

Para uma análise mais aprofundada sobre como mover sua implantação e preparar sua configuração local para migração, consulte Deployment Guide: Migrating Citrix Virtual Apps and Desktops from on-premises to Citrix Cloud na Tech Zone.

Baixar a Configuração Automatizada

Baixe e instale a ferramenta Automated Configuration do Citrix Downloads.

> **Importante:**
>
> Para evitar erros na funcionalidade, use sempre a versão mais recente disponível da Configuração Automatizada.

Atualizando a Configuração Automatizada

Ao executar cmdlets que acessam a nuvem na Configuração Automatizada, a ferramenta alerta quando há uma versão mais recente disponível para download.



Você pode ter certeza de que tem a versão mais recente seguindo as etapas abaixo:

1. Clique duas vezes no ícone **Configuração Automatizada**. Uma janela do PowerShell é exibida.
2. Execute o seguinte comando para verificar o número da versão.

   ```
   Get-CvadAcStatus
   ```

3. Verifique a versão da ferramenta em relação à versão listada no alerta ou em Citrix Downloads. A versão mais recente da ferramenta está localizada ali.
4. Baixe e instale a versão mais recente da ferramenta. Você *não* precisa desinstalar a versão antiga para atualizar a Configuração Automatizada.

> **Nota:**
>
> O alerta aparece sempre que você executa um cmdlet que acessa a nuvem. Para obter mais informações sobre cmdlets, consulte Cmdlets da ferramenta Automated Configuration.

Limitações conhecidas

- Os catálogos de máquinas provisionados por meio do Machine Creation Services têm considerações especiais. Para obter mais informações sobre o MCS, consulte Noções básicas sobre a migração de catálogos provisionados do Machine Creation Services.

Objetos de migração compatíveis

A Configuração Automatizada oferece suporte à movimentação da configuração dos seguintes componentes:

- Marcas
- Administrador delegado
  - Escopos
  - Funções
- Conexões de host
  - Um único pool de recursos
  - Escopos de administração
- Catálogos de máquinas
  - Escopos de administração
  - Máquinas
  - Acesso ao PC remoto, físico, em pool, provisionado, MCS, atribuído
- StoreFronts
- Grupos de entrega
  - Política de acesso
  - Associação de escopo de administração
  - Política de acesso a aplicativos
  - Política de atribuição
  - Política de direitos/área de trabalho
  - Programações de energia
  - Persistência de sessão

    - Pré-lançamento da sessão
    - Agendas de reinicialização
    - Marcas
- Grupos de aplicativos
    - Associação de escopo de administração
    - Grupos de entrega
    - Usuários e grupos
- Aplicativos
    - Pastas de aplicativos
    - Ícones
    - Aplicativos
    - FTAs configurados por agente
    - Marcas
- Políticas de grupo
- Preferências de zona de usuário

Ordem de migração de componentes

Os componentes e suas dependências estão listados aqui. As dependências de um componente devem existir antes que ele possa ser importado ou mesclado. Se uma dependência estiver ausente, isso pode fazer com que o comando import ou merge não funcione. A seção **Fixups** do arquivo de log mostra as dependências ausentes se uma importação ou mesclagem não funcionar.

1. Marcas
    - Sem pré-dependências
2. Administrador delegado
    - Sem pré-dependências
3. Conexões de host
    - Informações de segurança em CvadAcSecurity.yml

4. Catálogos de máquinas
    - Máquinas presentes no Active Directory
    - Conexões de host
    - Marcas
5. StoreFronts
6. Grupos de entrega
    - Máquinas presentes no Active Directory
    - Usuários presentes no Active Directory
    - Catálogos de máquinas
    - Marcas
7. Grupos de aplicativos
    - Grupos de entrega
    - Marcas
8. Aplicativos
    - Grupos de entrega
    - Grupos de aplicativos
    - Marcas
9. Políticas de grupo
    - Grupos de entrega
    - Marcas
10. Preferências de zona de usuário

Pré-requisitos comuns

A seguir estão alguns pré-requisitos comuns que são necessários para que a Configuração Automatizada funcione corretamente. Esses pré-requisitos são usados tanto em migrações locais para nuvem quanto de nuvem para nuvem.

Geração do ID do consumidor, o ID do cliente e a chave secreta

Antes de iniciar a migração usando a Configuração Automatizada, você precisa do seu ID de consumidor do Citrix Cloud e deve criar um ID de cliente e uma chave secreta para importar sua configuração para o Citrix Cloud. Todos os cmdlets que acessam a nuvem exigem esses valores.

As etapas a seguir permitem recuperar o ID de consumidor e criar o ID do cliente e a chave secreta.

Para recuperar a **ID do consumidor**:

1. Faça login na sua conta do Citrix Cloud e selecione o consumidor.

2. Clique no menu de hambúrguer e selecione **Identity and Access Management** no menu suspenso.

3. A **ID do consumidor** está localizada na página **Identity and Access Management**.

Para recuperar o **ID do cliente** e a **chave secreta**:

1. Na página **Identity and Access Management**, clique na guia **API Access**.

2. Digite um nome na caixa. Esse nome é usado para diferenciar entre vários IDs de cliente e chaves secretas. Clique em **Create Client** para criar o ID do cliente e a chave secreta.

3. A caixa de diálogo a seguir aparece depois que você cria com êxito o ID do cliente e a chave secreta. Tenha o cuidado de copiar os dois valores para um local seguro e baixar o arquivo.csv que contém essas informações. O arquivo .csv pode ser usado para criar o arquivo CustomerInfo.yml.

4. O ID do cliente e a chave secreta são criados com êxito.

Coloque esses valores em um local seguro e compartilhe somente com membros confiáveis da empresa que precisam acessar a ferramenta ou acessar as APIs Rest da nuvem. O ID do cliente e a chave secreta não expiram. Se eles forem comprometidos, remova-os imediatamente usando o ícone de **Lixeira** e crie novos.

> **Nota:**
>
> A chave secreta não pode ser recuperada se for perdida ou esquecida; devem ser criados um novo ID de cliente e chave secreta.

Preenchendo o arquivo de informações do cliente

O uso do arquivo CustomerInfo.yml elimina a necessidade de fornecer parâmetros de informações do cliente com a execução de cada cmdlet. Qualquer uma das informações do cliente pode ser substituída usando parâmetros de cmdlet.

Crie o arquivo CustomerInfo.yml usando o cmdlet `New-CvadAcCustomerInfoFile`.

> **Importante:**
>
> Não edite manualmente o arquivo CustomerInfo.yml. Isso pode causar erros de formatação inadvertidos.

> O `New-CvadAcCustomerInfoFile` tem os seguintes parâmetros obrigatórios.

- CustomerId — ID do consumidor.
- ClientId — ID do cliente do consumidor criado no Citrix Cloud.
- Secret — segredo do cliente criado no Citrix Cloud.

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId 6813EEA6-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaw==
```

Você também pode criar o CustomerInfo.yml usando o `SecurityCsvFileSpec` parâmetro que aponta para o arquivo security.csv baixado. Você também deve especificar o CustomerId.

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:\Users\my_user_name\downloads/security.csv -CustomerId markhof123
```

Atualize o arquivo CustomerInfo.yml usando o cmdlet `Set-CvadAcCustomerInfoFile`. Esse cmdlet altera apenas o ID do cliente.

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

Veja a seguir um exemplo de arquivo CustomerInfo.yml.

Created/Updated on 2020/01/29 16:46:47

```
CustomerId: 'markhof123'

ClientId: '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'

Secret: 'TwBLaaabbbaaaaaaaaaaw=='

Environment: Production

AltRootUrl: ''

StopOnError: False

AlternateFolder: ''

Locale: 'en-us'

Editor: 'C:\Program Files\Notepad++\notepad++.exe'

Confirm: True

DisplayLog: True
```

Preenchimento do arquivo de mapeamento de zona

Uma zona local é o equivalente ao local do recurso da nuvem. Ao contrário de outros componentes do site, você não pode importar a zona local para a nuvem automaticamente. Em vez disso, ele deve ser mapeado manualmente usando o arquivo ZoneMapping.yml. Falhas de importação podem ocorrer se o nome da zona não estiver associado a um nome de local de recursos existente.

Para sites locais com apenas uma zona e sites de nuvem apenas um local de recursos, a ferramenta Automated Configuration faz a associação correta, eliminando a necessidade de gerenciar manualmente o arquivo ZoneMapping.yml.

No caso de sites locais com várias zonas ou sites de nuvem com vários locais de recursos, o arquivo ZoneMapping.yml deve ser atualizado manualmente para refletir o mapeamento correto de zonas locais para locais de recursos na nuvem. Isso deve ser feito antes de tentar qualquer operação de importação para a nuvem.

O arquivo ZoneMapping.yml está localizado em *%HOMEPATH%\Documents\Citrix\AutoConfig*. O conteúdo do arquivo .yml é um dicionário com o nome da zona como chave e o nome do local do recurso como o valor.

Como exemplo, um site local do Citrix Virtual Apps and Desktops com uma zona primária chamada "Zone-1" e uma zona secundária chamada "Zone-2" é migrado para uma implantação do Citrix DaaS com dois locais de recursos de nuvem recém-criados chamados "Cloud-RL-1" e "Cloud-RL-2". Nesse caso, o ZoneMapping.yml seria configurado da seguinte forma:

```
Zone-1: Cloud-RL-1



Zone-2: Cloud-RL-2
```

Nota:

Deve haver um espaço entre os dois pontos e o nome do local do recurso. Se forem usados espaços na zona ou no nome do local do recurso, escreva o nome entre aspas.

Conexões de host

As conexões de host e seus hipervisores associados podem ser exportados e importados usando a Configuração Automatizada.

Adicionar um hipervisor a uma conexão de host requer informações de segurança específicas para o tipo de hipervisor. Essas informações não podem ser exportadas do site local por questões de segurança. Você deve fornecer as informações manualmente para que a Configuração Automatizada possa importar com êxito conexões de host e hipervisores para o site da nuvem.

O processo de exportação cria o arquivo CvadAcSecurity.yml em *%HOMEPATH%\Documents\Citrix\AutoConfig* contendo espaços reservados para cada item de segurança necessário para o tipo de hipervisor específico. Você deve atualizar o arquivo CvadAcSecurity.yml antes de importar para o site da nuvem. As atualizações do administrador são mantidas em várias

exportações com novos espaços reservados de segurança adicionados conforme necessário. Itens de segurança nunca são removidos. Para obter mais informações, consulte Atualizar manualmente o arquivo CvadAcSecurity.yml

```
HostConn1:

ConnectionType: XenServer

UserName: root

PasswordKey: rootPassword

HostCon2:

ConnectionType: AWS

ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH

SecretKey: TwBLaaaaaaaaaaaaaaaaw==

Region: East
```

Informações de segurança por hipervisor

O seguinte lista as informações de segurança necessárias para cada tipo de hipervisor.

- XenServer, Hyper-V, VMware
  - Nome de usuário
  - Senha com texto não criptografado
- Microsoft Azure
  - ID de assinatura
  - ID do aplicativo
  - Segredo do aplicativo
- Amazon Web Services
  - ID de conta de serviço
  - Segredo do aplicativo
  - Região

Considerações especiais de segurança

Todas as informações de segurança são inseridas como texto não criptografado. Se o texto não criptografado não for recomendado, as conexões de host e os hipervisores associados poderão ser criados manualmente usando a interface **Manage > Full Configuration**. As conexões de host e os nomes do hipervisor devem corresponder exatamente às suas contrapartes locais para que os catálogos de máquinas que usam as conexões de host possam ser importados com êxito.

Ativação de sites

O Delivery Controller em sites locais e na nuvem controla recursos como intermediação de desktops, aplicativos e reinicialização de máquinas. Os problemas ocorrem quando um conjunto comum de recursos é controlado por dois ou mais sites. Essa situação pode ocorrer ao migrar de um site local para um site na nuvem. É possível que os Delivery Controllers no local e na nuvem gerenciem o mesmo conjunto de recursos. Esse gerenciamento duplo pode fazer com que os recursos se tornem indisponíveis e incontroláveis, e pode ser difícil de diagnosticar.

A ativação do site permite que você controle onde o site ativo é controlado.

A ativação do site é gerenciada usando o modo de manutenção do grupo de entrega. Os grupos de entrega são colocados no modo de manutenção quando o site está inativo. O modo de manutenção é removido dos grupos de entrega para sites que estão ativos.

A ativação do site não afeta nem gerencia o registro do VDA ou os catálogos de máquinas.

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

Todos os cmdlets oferecem suporte à `IncludeByName` e à `ExcludeByName` filtragem. Esse parâmetro permite que você selecione quais grupos de entrega podem ter seu modo de manutenção alterado. Os grupos de entrega podem ser alterados seletivamente conforme necessário.

Importar e transferir o controle para a nuvem

Veja a seguir uma descrição de alto nível sobre como importar e transferir o controle do site local para o site na nuvem.

1. Exporte e importe o site local para a nuvem. Verifique se o parâmetro `–SiteActive` não está presente em nenhum dos cmdlets de importação. O site local está ativo e o site da nuvem inativo. Por padrão, os grupos de entrega de sites na nuvem estão no modo de manutenção.
2. Verifique o conteúdo e a configuração da nuvem.

3. Fora do horário de expediente, defina o site local como inativo. O parâmetro `–SiteActive` deve estar ausente. Todos os grupos de entrega no local estão em modo de manutenção.
    - `Set-CvadAcSiteActiveStateOnPrem`
4. Defina o site da nuvem como ativo. O parâmetro `–SiteActive` deve estar presente. Nenhum grupo de entrega de site na nuvem está no modo de manutenção.
    - `Set-CvadAcSiteActiveStateCloud –SiteActive`
5. Verifique se o site da nuvem está ativo e se o site local está inativo.

Transferência do controle de volta para o site local

Para transferir o controle do site da nuvem para o site local:

1. Durante o horário de folga, defina o site da nuvem como inativo. Todos os grupos de entrega de sites em nuvem estão em modo de manutenção.
    - `Set-CvadAcSiteActiveStateCloud`
2. Defina o site local como ativo. Nenhum grupo de entrega no local está em modo de manutenção.
    - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

Informações adicionais sobre ativação do site

- Se nenhuma máquina tiver gerenciamento de energia e não houver agendamentos de reinicialização (o que geralmente significa que também não há conexões de host), todos os grupos de entrega na nuvem podem ser importados como ativos. Adicione `-SiteActive` a `Merge-CvadAcToSite` / `Import-CvadAcToSite` ou execute `Set-CvadAcSiteActiveStateCloud -SiteActive` após a importação.
- Se as máquinas tiverem gerenciamento de energia ou houver agendamentos de reinicialização, será necessário um processo diferente. Por exemplo, ao alternar do local para a nuvem nessa situação, defina o site local como inativo usando `Set-CvadAcSiteActiveStateOnPrem`. Em seguida, defina o site da nuvem como ativo usando `Set-CvadAcSiteActiveStateCloud -SiteActive`.
- O cmdlets `Set-CvadAcSiteActiveStateCloud` e `Set-CvadAcSiteActiveStateOnPrem` também são usados para reverter o processo. Por exemplo, execute `Set-CvadAcSiteActiveStateCloud` sem o parâmetro `-SiteActive` e, em seguida, execute `Set-CvadAcSiteActiveStateOnPrem` com o parâmetro `-SiteActive`.

Como é a migração de catálogos provisionados do Machine Creation Services

> **Nota:**
>
> Esse recurso está disponível somente nas versões 3.0 e posteriores. Verifique sua versão usando `Get-CvadAcStatus` na Configuração Automatizada.

> Os catálogos do Machine Creation Services (MCS) criam dois tipos diferentes de catálogos:

- Quando as alterações feitas em uma máquina são perdidas/revertidas (normalmente OS Server, onde os aplicativos são publicados) — este é um caso de uso de VDI em pool/ multissessão
- Quando as alterações feitas em uma máquina são preservadas durante a reinicialização (geralmente sistema operacional cliente com um usuário dedicado) — este é um caso de uso estático de VDI

O tipo de catálogo pode ser confirmado no nó do catálogo no Citrix Studio e com base no valor "User data:" do catálogo.

> **Nota:**
>
> Não é possível fazer backup do MCS da nuvem usando a Configuração Automatizada.

Catálogos VDI/multissessão em pool

Catálogos com "User data: Discard" são catálogos VDI em pool e só podem migrar a imagem principal e a configuração. As máquinas virtuais nesses catálogos não são migradas. Isso ocorre porque o ciclo de vida da máquina virtual é mantido pelo site do qual você está importando, o que significa que toda vez que as máquinas são ligadas, seu estado pode mudar. Isso torna a importação impossível, pois os dados de importação para as máquinas virtuais ficam rapidamente fora de sincronia.

Quando você está migrando esses catálogos usando a ferramenta, ela cria metadados de catálogo e inicia a criação da imagem principal, mas nenhuma máquina é importada.

Como esse processo pode levar algum tempo para ser criado com base no tamanho da imagem principal, o comando import dentro da ferramenta apenas inicia a criação do catálogo MCS e não espera que ele termine. Após a conclusão da importação, monitore o progresso da criação do catálogo usando a interface de gerenciamento Full Configuration na implantação da nuvem.

Depois que a imagem principal for criada, você poderá provisionar máquinas. As considerações de capacidade precisam ser levadas em consideração, pois você teria capacidade consumida pelo uso local.

Todos os outros objetos (grupos de entrega/aplicativos/políticas e assim por diante) que usam esse catálogo podem ser importados e não precisam aguardar a criação da imagem principal. Quando o catálogo terminar de criar, as máquinas poderão ser adicionadas ao catálogo importado e, em seguida, os usuários poderão iniciar seus recursos.

> **Nota:**
>
> Use os mesmos comandos disponíveis na ferramenta para migrar catálogos e todos os outros objetos.

Catálogos VDI estáticos

> **Nota:**
>
> Como essa operação importa detalhes de baixo nível armazenados no banco de dados, esse processo deve ser executado em uma máquina com acesso ao banco de dados.
>
> Os catálogos VDI estáticos migram a imagem principal, as configurações e todas as máquinas virtuais. Ao contrário do caso de uso de VDI em pool, nenhuma imagem precisa ser criada.

Os VDAs devem ser apontados para o conector para que eles se registrem na nuvem.

Consulte a seção Ativação de sites para tornar o site na nuvem ativo, de modo que o cronograma de reinicialização, o gerenciamento de energia e outros itens sejam controlados pela nuvem.

Quando a migração for concluída, se você quiser excluir esse catálogo do site local, selecione sair da VM e da conta do AD. Caso contrário, eles serão excluídos e o site da nuvem será deixado apontando para a VM excluída.

Cmdlets da ferramenta de configuração automatizada

Esta página lista todos os cmdlets e parâmetros suportados pela ferramenta.

Todos os cmdlets adotam parâmetros com um dos seguintes tipos.

- Cadeia de caracteres
- Lista de cadeias de caracteres
- Booleano: `$true` ou `$false`
- SwitchParameter: presença das médias dos parâmetros `$true`; ausência das médias dos parâmetros `$false`

> **Nota:**
>
> SwitchParameter é o método preferido para seleções verdadeiras ou falsas, mas os booleanos ainda são usados na ferramenta devido a problemas de legado.

> A tabela a seguir é um resumo de todos os cmdlets. Consulte cada seção individual para descobrir quais parâmetros cada cmdlet oferece suporte.

CATEGORIA	CMDLET	DESCRIÇÃO
Migração de local para nuvem	`Export-CvadAcToFile`	Exportar arquivos locais para arquivos YAML.
	`Import-CvadAcToSite`	Importar arquivos YAML para a nuvem. Suporta operações de criação, atualização e exclusão.
	`Merge-CvadAcToSite`	Importar arquivos YAML para a nuvem. Oferece suporte a operações de criação e atualização.

CATEGORIA	CMDLET	DESCRIÇÃO
	`New-CvadAcToSite`	Importar arquivos YAML para a nuvem. Suporta somente operações de criação.
	`Sync-CvadAcToSite`	Exportar e importar em uma única etapa.
	Migração granular No caso de componentes, use parâmetros com os comandos acima. Exemplos: `MachineCatalogs`, `Tags`. No caso de nomes de componentes, use parâmetros com os comandos acima. Exemplos: `IncludeByName`, `ExcludeByName`.	Migrar seletivamente apenas componentes ou nomes de componentes
Cmdlets de nuvem para nuvem	`Backup-CvadAcToFile`	Faz backup de toda a configuração do seu site na nuvem.
	`Restore-CvadAcToSite`	Restaura arquivos YAML de backup para o site da nuvem. Esse site na nuvem pode ser igual ou diferente do site de nuvem de origem.
	`Remove-CvadAcFromSite`	Remova membros do componente da nuvem.
	Migração granular No caso de componentes, use parâmetros com os comandos acima. Exemplos: `MachineCatalogs`, `Tags`. No caso de nomes de componentes, use parâmetros com os comandos acima. Exemplos:	Migrar seletivamente apenas componentes ou nomes de componentes

CATEGORIA	CMDLET	DESCRIÇÃO
	`IncludeByName`, `ExcludeByName`.	
Outros cmdlets básicos	`Compare-CvadAcToSite`	Compara os arquivos .yml locais com a configuração da nuvem.
Cmdlets relacionados a pré-requisitos	`New-CvadAcCustomerInfoFile`	Criar um arquivo de informações do consumidor.
	`Set-CvadAcCustomerInfoFile`	Atualizar um arquivo de informações do consumidor existente.
Cmdlets de suporte e solução de problemas	`New-CvadAcZipInfoForSupport`	Compacta todos os arquivos de log e .yml em um único arquivo zip para enviar à Citrix para suporte.
	`Get-CvadAcStatus`	Use para testar a conectividade e garantir que todos os pré-requisitos sejam atendidos. Retorna informações sobre a ferramenta, como número da versão e conectividade com a nuvem e o status do conector.
	`Test-CvadAcConnectionWithSite`	Teste a conexão com o site da nuvem.
	`Find-CvadAcConnector`	Localiza os conectores existentes e determina seu estado de execução.
	`Get-CvadAcCustomerSites`	Retorna a lista de todos os sites de consumidores.

CATEGORIA	CMDLET	DESCRIÇÃO
	`New-CvadAcTemplateToFile`	Cria um arquivo de modelo para componentes selecionados.
	`Show-CvadAcDocument`	Exibe essa documentação no navegador padrão.
	`Find-CvadAcInFile`	Localizar no componente de pesquisas de arquivos YAML procurando membros que correspondam a um ou mais nomes que possam conter curingas.
Cmdlets de ativação do site	`Set-CvadAcSiteActiveStateOnPrem`	Define o estado do site local como ativo ou inativo.
	`Set-CvadAcSiteActiveStateCloud`	Define o estado do site da nuvem como ativo ou inativo.
Mesclagem de vários cmdlets de sites locais	`New-CvadAcSiteMergingInfo`	Cria um conjunto de informações de prefixo/sufixo de mesclagem de sites.
	`Set-CvadAcSiteMergingInfo`	Atualiza um conjunto de informações de prefixo/sufixo de mesclagem de sites existente.
	`Remove-CvadAcSiteMergingInfo`	Remove um conjunto de informações de prefixo/sufixo de mesclagem de site existente.

Para obter mais informações sobre parâmetros e como usá-los, consulte Parâmetros de migração granular.

Cmdlets básicos

Cmdlets locais para a nuvem

- `Export-CvadAcToFile` - Exportar arquivos locais para arquivos YAML.

  Exporta a configuração da configuração local. Essa é a operação de exportação padrão para a Configuração automatizada. Nenhuma modificação é feita na configuração do site local. Os arquivos exportados são colocados no diretório *%HOMEPATH%\Documents\Citrix\AutoConfig* em uma subpasta **Export** com nome exclusivo. A pasta *%HOMEPATH%\Documents\Citrix\AutoConfig* sempre contém a configuração de site local exportada mais recente.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes		SwitchParameters
Filtrar por nomes de objetos	Consulte Filtragem por nomes de objetos		Lista de cadeias de caracteres
`TargetFolder`	Especifica a pasta de destino da exportação.		Cadeia de caracteres
`Locale`	Especifica o idioma do texto legível por seres humanos que pode ser exportado.		Cadeia de caracteres
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`AdminAddress`	Especifica o DNS ou o endereço IP do Delivery Controller quando a exportação não está sendo executada no		Cadeia de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	Controlador de Entrega.		
`CheckUserAndMachines`	Verifica se os usuários e as máquinas estão no Active Directory. Usuários e máquinas que não estão no Active Directory podem resultar em falhas de importação.		`$true` ou `$false`
`ZipResults`	Compacta o backup de arquivos YAML em um único arquivo zip. O arquivo está na mesma pasta que os arquivos YAML de backup e tem o mesmo nome da pasta.		SwitchParameter

Retorna:

- Consulte Valores de retorno do cmdlet

Existem três maneiras de importar dados para a nuvem. A execução de cmdlets específicos pode resultar em uma das três combinações de ações no site da nuvem:

- Adicionar, atualizar e excluir
- Adicionar e atualizar somente
- Adicionar apenas

CMDLET	ADICIONAR	ATUALIZAR	DELETE
Importar	X	X	X

CMDLET	ADICIONAR	ATUALIZAR	DELETE
Mesclar	X	X	
Novo	X		

- `Import-CvadAcToSite` - Importar arquivos YAML para a nuvem. Suporta operações de criação, atualização e exclusão.

  Importa todos os arquivos locais para a nuvem. Esse comando garante que o estado final da nuvem seja idêntico ao estado local. Essa opção exclui todas as alterações existentes na nuvem. Os arquivos de configuração de site importados são provenientes de *%HOMEPATH%\Documents\Citrix\AutoConfig*. *Use com cuidado.*

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes.		SwitchParameters
Filtrar por nomes de objetos	Consulte Filtragem por nomes de objetos.		Lista de cadeias de caracteres
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters
`SourceFolder`	Identifica uma pasta raiz substituta para *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Cadeia de caracteres
`Locale`	Especifica o idioma do texto legível por seres humanos que pode ser exportado.		Cadeia de caracteres
`Quiet`	Suprimir o registro em log no console.		SwitchParameter

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`Merge`	Quando definido como `$true`, só adiciona componentes ao site da nuvem. Os componentes não são removidos. Defina como `$false` para remover componentes.		`$true` ou `$false`
`AddOnly`	Quando definido como `$true`, adiciona apenas novos componentes, não atualiza nem exclui componentes existentes. Defina como `$false` para permitir atualizações e exclusões. `Merge` é ignorado quando esse parâmetro é `$true`.		`$true` ou `$false`
`MergePolicies`	Mesclar configurações de política e filtros. A mesclagem ocorre somente quando uma política que		SwitchParameter

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	está sendo importada já existe no DDC da nuvem. O resultado da mesclagem de políticas é que as políticas de nuvem DDC contêm as configurações e os filtros que já tinham, além das novas configurações e filtros que estão sendo importados. Observe que, quando ocorrem colisões de configuração e filtro, os valores importados têm precedência.		
`OnErrorAction`	Consulte Parâmetro OnErrorAction.		Cadeia de caracteres

Retorna:

- Consulte Valores de retorno do cmdlet

- `Merge-CvadAcToSite` - Importar arquivos YAML para a nuvem. Oferece suporte a operações de criação e atualização.

  Mescla os arquivos locais com a nuvem, mas *não* exclui nenhum componente na nuvem ou no site local. Isso preserva as alterações já feitas na nuvem. Se existir um componente no Citrix Cloud com o mesmo nome, esse comando poderá modificar esse componente. Essa é a operação de importação padrão para a Configuração automatizada. Os arquivos de configuração de site mesclados são provenientes de *%HOMEPATH%\Documents\Citrix\AutoConfig*.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes.		SwitchParameters
Filtrar por nomes de objetos	Consulte Filtragem por nomes de objetos.		Lista de cadeias de caracteres
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters
`SourceFolder`	Identifica uma pasta raiz substituta para *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Cadeia de caracteres
`Locale`	Especifica o idioma do texto legível por seres humanos que pode ser exportado.		Cadeia de caracteres
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`Merge`	Quando definido como `$true`, só adiciona componentes ao site da nuvem. Os componentes não são removidos. Defina como `$false` para		`$true` ou `$false`

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	remover componentes.		
`AddOnly`	Quando definido como `$true`, adiciona apenas novos componentes, não atualiza nem exclui componentes existentes. Defina como `$false` para permitir atualizações e exclusões. `Merge` é ignorado quando esse parâmetro é `$true`.		`$true` ou `$false`
`MergePolicies`	Mesclar configurações de política e filtros. A mesclagem ocorre somente quando uma política que está sendo importada já existe no DDC da nuvem. O resultado da mesclagem de políticas é que as políticas de nuvem DDC contêm as configurações e os filtros que já tinham, além das novas configurações e filtros que estão sendo importados. Observe que, quando ocorrem		SwitchParameter

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	colisões de configuração e filtro, os valores importados têm precedência.		
`OnErrorAction`	Consulte Parâmetro OnErrorAction.		Cadeia de caracteres

Retorna:

- Consulte Valores de retorno do cmdlet

- `New-CvadAcToSite` - Importar arquivos YAML para a nuvem. Oferece suporte a operações de criação e atualização.

  Importa a configuração do site local para a nuvem, mas adiciona apenas novos componentes. Os componentes existentes do site na nuvem não são atualizados nem excluídos. Use esse comando se for necessário que os componentes do site de nuvem existentes permaneçam inalterados.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes.		SwitchParameters
Filtrar por nomes de objetos	Consulte Filtragem por nomes de objetos.		Lista de cadeias de caracteres
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters
`SourceFolder`	Identifica uma pasta raiz substituta para *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Cadeia de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`Locale`	Especifica o idioma do texto legível por seres humanos que pode ser exportado.		Cadeia de caracteres
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`OnErrorAction`	Consulte Parâmetro OnErrorAction.		Cadeia de caracteres

Retorna:

- Consulte Valores de retorno do cmdlet

- `Sync-CvadAcToSite` - Exportar e importar em uma única etapa.

  A sincronização executa a exportação e a importação em uma única etapa. Use o parâmetro `SourceTargetFolder` para especificar a pasta de destino de exportação/importação.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes		SwitchParameters
Filtrar por nomes de objetos	Consulte Filtragem por nomes de objetos		Lista de cadeias de caracteres
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`SourceTargetFolder`	Especifica a pasta de destino de exportação/ importação.		Cadeia de caracteres
`Locale`	Especifica o idioma do texto legível por seres humanos que pode ser exportado.		Cadeia de caracteres
`AdminAddress`	Especifica o DNS ou o endereço IP do controlador de entrega quando a exportação não está sendo executada no controlador de entrega.		Cadeia de caracteres
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`Merge`	Quando definido como `$true`, só adiciona componentes ao site da nuvem. Os componentes não são removidos. Defina como `$false` para remover componentes.		`$true` ou `$false`

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`AddOnly`	Quando definido como `$true`, adiciona apenas novos componentes, não atualiza nem exclui componentes existentes. Defina como `$false` para permitir atualizações e exclusões. `Merge` é ignorado quando esse parâmetro é `$true`.		`$true` ou `$false`
`MergePolicies`	Mesclar configurações de política e filtros. A mesclagem ocorre somente quando uma política que está sendo importada já existe no DDC da nuvem. O resultado da mesclagem de políticas é que as políticas de nuvem DDC contêm as configurações e os filtros que já tinham, além das novas configurações e filtros que estão sendo importados. Observe que, quando ocorrem colisões de configuração e filtro, os valores		SwitchParameter

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	importados têm precedência.		

Retorna:

- Consulte Valores de retorno do cmdlet

Cmdlets de nuvem para nuvem

- `Backup-CvadAcToFile` - Faz backup de toda a configuração do seu site na nuvem.

  Exporta a configuração da nuvem para arquivos .yml. Esse backup pode ser usado em um processo de backup e restauração para restaurar componentes perdidos.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes		SwitchParameters
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`TargetFolder`	Especifica a pasta de destino da exportação.		Cadeia de caracteres
`Locale`	Especifica o idioma do texto legível por seres humanos que pode ser exportado.		Cadeia de caracteres
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false`		`$true` ou `$false`

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	para suprimir a exibição do log.		
`ZipResults`	Compacta o backup de arquivos YAML em um único arquivo zip. O arquivo está na mesma pasta que os arquivos YAML de backup e tem o mesmo nome da pasta.		SwitchParameter

Retorna:

- Consulte Valores de retorno do cmdlet

- `Restore-CvadAcToSite` - Restaura arquivos YAML de backup para o site da nuvem. Esse site na nuvem pode ser igual ou diferente do site de nuvem de origem.

  Restaura o site da nuvem para a configuração anterior. Os arquivos importados são originados da pasta especificada usando o parâmetro `-RestoreFolder`, que identifica a pasta que contém os arquivos .yml que devem ser restaurados no site da nuvem. Essa deve ser uma especificação de pasta totalmente qualificada. Esse cmdlet pode ser usado para reverter para a configuração anterior ou para fazer backup e restaurar seu site na nuvem. Esse comando pode adicionar, excluir e atualizar seu site na nuvem.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes.		SwitchParameters
Filtrar por nomes de objetos	Consulte Filtragem por nomes de objetos.		Lista de cadeias de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters
`RestoreFolder`	Identifica a pasta que contém os arquivos .yml que devem ser restaurados no site da nuvem. Essa deve ser uma especificação de pasta totalmente qualificada.		Cadeia de caracteres
`Locale`	Especifica o idioma do texto legível por seres humanos que pode ser exportado.		Cadeia de caracteres
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`
`Merge`	Quando definido como `$true`, só adiciona componentes ao site da nuvem. Os componentes não são removidos. Defina como `$false` para remover componentes.		`$true` ou `$false`

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`AddOnly`	Quando definido como `$true`, adiciona apenas novos componentes, não atualiza nem exclui componentes existentes. Defina como `$false` para permitir atualizações e exclusões. `Merge` é ignorado quando esse parâmetro é `$true`.		`$true` ou `$false`
`MergePolicies`	Mesclar configurações de política e filtros. A mesclagem ocorre somente quando uma política que está sendo importada já existe no DDC da nuvem. O resultado da mesclagem de políticas é que as políticas de nuvem DDC contêm as configurações e os filtros que já tinham, além das novas configurações e filtros que estão sendo importados. Observe que, quando ocorrem colisões de configuração e filtro, os valores		SwitchParameter

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	importados têm precedência.		
`OnErrorAction`	Consulte Parâmetro OnErrorAction.		Cadeia de caracteres

Retorna:

- Consulte Valores de retorno do cmdlet

- `Remove-CvadAcFromSite` — Remover membros do componente da nuvem.

  Pode redefinir o site inteiro ou remover itens de membro de um componente (por exemplo, remover um catálogo de máquina da lista de catálogos). Isso pode ser usado quando acoplado ao parâmetro `IncludeByName` para remover seletivamente membros específicos.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes		SwitchParameters
Filtrar por nomes de objetos	Consulte Filtragem por nomes de objetos		Lista de cadeias de caracteres
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`

Retorna:

- Consulte Valores de retorno do cmdlet

Outros cmdlets básicos

- `Compare-CvadAcToSite` - Compara os arquivos .yml locais com a configuração da nuvem, produzindo um relatório de alterações feitas por um cmdlet `Import`, `Merge` ou `Restore`.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes.		SwitchParameters
Filtrar por nomes de objetos	Consulte Filtragem por nomes de objetos.		Lista de cadeias de caracteres
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem.		SwitchParameters
`SourceFolder`	Identifica uma pasta raiz substituta para *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Cadeia de caracteres
`Locale`	Especifica o idioma do texto legível por seres humanos que pode ser exportado.		Cadeia de caracteres
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false` para suprimir a exibição do log.		`$true` ou `$false`

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`Merge`	Quando definido como `$true`, só adiciona componentes ao site da nuvem. Os componentes não são removidos. Defina como `$false` para remover componentes.		`$true` ou `$false`
`AddOnly`	Quando definido como `$true`, adiciona apenas novos componentes, não atualiza nem exclui componentes existentes. Defina como `$false` para permitir atualizações e exclusões. `Merge` é ignorado quando esse parâmetro é `$true`.		`$true` ou `$false`
`OnErrorAction`	Consulte Parâmetro OnErrorAction.		Cadeia de caracteres

Retorna:

- Consulte Valores de retorno do cmdlet

Parâmetros de migração granular

Migrar por componentes

Os seguintes componentes podem ser especificados com cmdlets que os suportam. A opção `All` é selecionada automaticamente quando não é especificado nenhum parâmetro de componente. Para evitar erros, recomendamos que você migre os componentes na seguinte ordem:

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

Filtrar por nomes de objetos

MIGRAR POR NOMES DE COMPONENTES

Os `ExcludeByName` parâmetros `IncludeByName` e permitem incluir e excluir membros de componentes em cmdlets por nome. Apenas um componente (por exemplo, grupos de entrega) pode ser escolhido por vez em qualquer um dos cmdlets suportados. Se um membro do componente estiver em ambas as áreas, a exclusão substituirá qualquer outro parâmetro e será criada uma entrada na lista de correção de log para identificar o componente e o nome do membro que foi excluído.

`IncludeByName` e `ExcludeByName` obtêm uma lista de nomes de membros de componentes. Qualquer nome pode conter um ou mais curingas. Dois tipos de curingas têm suporte. A lista de

nomes de membros de componentes deve estar entre aspas simples quando qualquer nome de membro contiver caracteres especiais.

- * Corresponde a qualquer número de caracteres
- ? Corresponde a um único caractere

`IncludeByName` e `ExcludeByName` também podem obter um arquivo que contém uma lista de membros em que cada membro pode ser explícito ou conter curingas. Cada linha do arquivo pode conter um membro. Os espaços à esquerda e à direita são cortados do nome do membro. O nome do arquivo deve ser precedido pelo sinal @ e estar entre aspas simples (um requisito do PowerShell para que o @ não seja reinterpretado). Podem ser listados vários arquivos, que também podem ser misturados com nomes de membros.

Um exemplo de mesclagem de todos os grupos de entrega cujos nomes começam com `DgSite1` e contêm `Home2` seria escrito:

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

POR NOME DO GRUPO DE ENTREGA

`ByDeliveryGroupName` filtra pelo nome do grupo de entrega para aplicativos e grupos de aplicativos. Esse parâmetro é sempre uma lista de inclusão que identifica os membros a serem incluídos com base na associação do grupo de entrega.

`ByDeliveryGroupName` pega uma lista de nomes de grupos de entrega. Qualquer nome pode conter um ou mais curingas. Dois tipos de curingas têm suporte.

- * corresponde a qualquer número de caracteres
- ? corresponde a um único caractere

O exemplo a seguir mescla todos os aplicativos que fazem referência a todos os nomes de grupos de entrega que começam com `EastDg`.

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

EXCLUIR DESATIVADO

`ExcludeDisabled` filtra das operações de importação todos os aplicativos e grupos de aplicativos que estão desativados. `ExcludeDisabled` passa para o valor padrão `false`, o que significa que todos os aplicativos e grupos de aplicativos são importados independentemente do estado ativado.

POR NOME DE MÁQUINA

`ByMachineName` filtra pelo nome da máquina para catálogos de máquinas e grupos de entrega. Esse parâmetro é sempre uma lista de inclusão que identifica os membros a serem incluídos com base na associação de nomes de máquinas.

`ByMachineName` usa uma lista de nomes de máquinas em que qualquer nome pode conter um ou mais curingas. Dois tipos de curingas têm suporte.

- * corresponde a qualquer número de caracteres
- ? corresponde a um único caractere

Ao exportar ou importar e usar `ByMachineName` e um filtro de nome de máquina não resultar em máquinas no catálogo de máquinas ou no grupo de entrega, o catálogo de máquinas ou o grupo de entrega é excluído da exportação ou importação.

> **Nota:**
>
> O uso de `ByMachineName` em qualquer tipo de cmdlet de importação resulta em `MergeMachines` definido como `$true`.

MESCLAR MÁQUINAS

`MergeMachines`, quando definido como `$true`, instrui a operação de importação a adicionar máquinas somente ao catálogo de máquinas ou ao grupo de entrega. As máquinas não são removidas, permitindo operações aditivas incrementais.

`MergeMachines` o padrão é falso, o que significa que as máquinas são removidas se não estiverem presentes no catálogo de máquinas ou no arquivo .yml do grupo de entrega. `MergeMachines` está definido como `$true` quando `ByMachineName` é usado, mas pode ser substituído definindo como `MergeMachines` false.

Cmdlets relacionados a pré-requisitos

- `New-CvadAcCustomerInfoFile` - Crie um arquivo de informações do consumidor. Por padrão, o arquivo de informações do consumidor está localizado em *%HOMEPATH%\Documents\Citrix\AutoConfig*.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`CustomerId`	ID do consumidor.	x	Cadeia de caracteres
`ClientId`	ID de consumidor do consumidor criado no Citrix Cloud. O CustomerID e o Secret devem ser especificados ao usar esse parâmetro.	Condicionalmente	Cadeia de caracteres
`Secret`	Chave secreta do consumidor criada no Citrix Cloud. O CustomerID e o ClientID devem ser especificados ao usar esse parâmetro.	Condicionalmente	Cadeia de caracteres
`Environment`	Ambiente Production, ProductionGov ou ProductionJP.		Enumeração
`LogFileName`	Altere o prefixo do arquivo de log do CitrixLog para outra coisa.		Cadeia de caracteres
`AltRootUrl`	Use somente sob a direção da Citrix.		Cadeia de caracteres
`StopOnError`	Interrompe a operação no primeiro erro.		`$true` ou `$false`
`TargetFolder`	Use a pasta especificada como		Cadeia de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	a pasta raiz em vez de *%HOMEPATH%\Documents\Citrix\AutoConfig*.		
`Locale`	Use o local especificado em vez da localidade derivada do sistema em que a ferramenta é executada.		Cadeia de caracteres
`Editor`	Use o editor especificado para exibir o log na conclusão de cada cmdlet. O Notepad.exe é o editor padrão. Esse parâmetro deve incluir a especificação de arquivo totalmente qualificada para o editor e o editor deve tomar a especificação do arquivo de log como seu único parâmetro.		Cadeia de caracteres
`SecurityCsvFileSpec`	A especificação de arquivo totalmente qualificada que aponta para o arquivo SecurityClient.csv baixado do Citrix Identity and Access Management. O		Cadeia de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	CustomerID deve ser especificado quando esse parâmetro é usado.		

Retorna:

- Consulte Valores de retorno do cmdlet

- `Set-CvadAcCustomerInfoFile` - Atualize um arquivo de informações do consumidor existente. Somente os parâmetros especificados pelo cmdlet são alterados. Todos os valores de parâmetros não especificados no arquivo CustomerInfo.yml permanecem inalterados.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`CustomerId`	ID do consumidor.		Cadeia de caracteres
`ClientId`	ID de consumidor do consumidor criado no Citrix Cloud.		Cadeia de caracteres
`Secret`	Chave secreta do consumidor criada no Citrix Cloud.		Cadeia de caracteres
`Environment`	Ambiente Production, ProductionGov ou ProductionJP.		Enumeração
`LogFileName`	Altere o prefixo do arquivo de log do CitrixLog para outra coisa.		Cadeia de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`StopOnError`	Interrompe a operação no primeiro erro.		`$true` ou `$false`
`TargetFolder`	Use a pasta especificada como a pasta raiz em vez de *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Cadeia de caracteres
`Locale`	Use o local especificado em vez da localidade derivada do sistema em que a ferramenta é executada.		Cadeia de caracteres
`Editor`	Use o editor especificado para exibir o log na conclusão de cada cmdlet. O Notepad.exe é o editor padrão. Esse parâmetro deve incluir a especificação de arquivo totalmente qualificada para o editor e o editor deve tomar a especificação do arquivo de log como seu único parâmetro.		Cadeia de caracteres
`SecurityCsvFileSpec`	A especificação de arquivo totalmente qualificada que		Cadeia de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	aponta para o arquivo SecurityClient.csv baixado do Citrix Identity and Access Management. O CustomerID deve ser especificado quando esse parâmetro é usado.		

Retorna:

- Consulte Valores de retorno do cmdlet

Parâmetros relacionados aos pré-requisitos

Junto com os parâmetros de acesso à nuvem, os seguintes parâmetros podem ser usados com os cmdlets relacionados aos pré-requisitos:

- `Environment` – Ambiente Production ou ProductionGov.
- `LogFileName` – Altere o prefixo do arquivo de log do CitrixLog para outra coisa.
- `StopOnError` – Interrompe a operação no primeiro erro.
- `AlternateRootFolder` – Usar a pasta especificada como a pasta raiz em vez de *%HOMEPATH%\Documents\Citrix\AutoConfig*.
- `Locale` – Usar o local especificado em vez da localidade derivada do sistema em que a ferramenta é executada.
- `Editor` – Usar o editor especificado para exibir o log na conclusão de cada cmdlet. O Notepad.exe é o editor padrão. Esse parâmetro deve incluir a especificação de arquivo totalmente qualificada para o editor e o editor deve tomar a especificação do arquivo de log como seu único parâmetro.

Cmdlets de suporte e solução de problemas

- `New-CvadAcZipInfoForSupport` - Compacta todos os arquivos de log e .yml em um único arquivo zip para enviar à Citrix para suporte. Informações confidenciais do consumidor (CustomerInfo.yml e CvadAcSecurity.yml) não estão incluídas no zip. O arquivo Icon.yml também é excluído devido ao seu tamanho. O arquivo zip é colocado em *%HOMEPATH%*

\Documents\Citrix\AutoConfig e nomeado *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, com base na data e no carimbo de data/hora. Esse arquivo zip também pode funcionar como um backup.

Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`TargetFolder`	Especifica uma pasta de destino para criar e salvar o arquivo zip.		Cadeia de caracteres
`Quiet`	Suprimir o registro em log no console.		SwitchParameter

Retorna:

- O arquivo zip com o nome e a localização é exibido no prompt de comando.

- `Get-CvadAcStatus` - Use para testar a conectividade e garantir que todos os pré-requisitos sejam atendidos. Retorna informações sobre a ferramenta, como número da versão e conectividade com a nuvem e o status do conector.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`SiteId`	Identifica o site ao qual se conectar.		Cadeia de caracteres
`AdminAddress`	Este é o endereço DNS ou IP do Delivery Controller local usado para verificar o nível de acesso do administrador. Isso é necessário se a		Cadeia de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	ferramenta não estiver sendo executada em um Delivery Controller.		

Retorna:

- Exibe os resultados de cada item.

- `Test-CvadAcConnectionWithSite` — Teste a conexão com o site da nuvem para verificar se a conexão de comunicação está funcionando. Esse cmdlet usa os parâmetros de acesso à nuvem ou o arquivo CustomerInfo.yml para especificar as informações de conexão do consumidor.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`Quiet`	Suprimir o registro em log no console.		SwitchParameter

  Retorna:

  - Os resultados do teste são exibidos na linha de comando.

- `Find-CvadAcConnector` - Localiza os conectores existentes e determina seu estado de execução. Esse cmdlet usa informações do arquivo CustomerInfo.yml ou do parâmetro de ID do cliente para localizar os conectores do consumidor.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`CustomerInfoFileSpec`	A especificação do arquivo que aponta para um arquivo de informações do		Cadeia de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	consumidor para substituir o local e o nome padrão. Esse parâmetro é ignorado quando é fornecido o parâmetro `CustomerId`.		
`CustomerId`	O ID do consumidor. Esse parâmetro substitui o mesmo valor no arquivo CustomerInfo.yml.		Cadeia de caracteres

Retorna:

- Os resultados são mostrados na linha de comando.

- `Get-CvadAcCustomerSites` - Retorna a lista de todos os sites dos consumidores. Esse cmdlet usa os parâmetros de acesso à nuvem ou o arquivo CustomerInfo.yml para especificar as informações de conexão do consumidor.

  Parâmetros:

  - Consulte Parâmetros de acesso à nuvem

  Retorna:

  - Exibe uma lista de IDs de sites de consumidor encontrados.

- `New-CvadAcTemplateToFile` – Cria um arquivo de modelo para componentes selecionados, permitindo que você crie manualmente um arquivo de importação.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes		SwitchParameters

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`TargetFolder`	Especifica a pasta de destino da exportação.		Cadeia de caracteres

Retorna:

- Consulte Valores de retorno do cmdlet

- `Show-CvadAcDocument` - Exibe esta documentação no navegador padrão.

  Parâmetros:

  - Nenhuma.

  Retorna:

  - Exibir esta página da Web no navegador da Web padrão.

- `Find-CvadAcInFile` - Encontrar no componente de pesquisas de arquivos YAML procurando membros que correspondam a um ou mais nomes que possam conter curingas. O resultado é um relatório de membros encontrados. Localizar no arquivo só pode pesquisar um componente por vez. Localizar no arquivo pesquisa todos os arquivos YAML na pasta atual e em todas as subpastas. Use `FindSourceFolder` para limitar o número de arquivos a serem pesquisados.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Migrar por componentes	Consulte Migrar por componentes. Nota: O valor `-All` não é válido.		SwitchParameters
`IncludeByName`	Uma lista que especifica os nomes dos grupos de entrega que devem ser incluídos ao definir o estado ativo do site como		Lista de cadeias de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	ativo. Os caracteres curinga '*' e '?' são suportados em nomes.		
`Unique`	Indicar apenas membros encontrados exclusivamente.		SwitchParameter
`IncludeYaml`	Inclua o YAML específico do membro.		SwitchParameter
`FindSourceFolder`	A pasta em que a função de busca começa.		Cadeia de caracteres
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false` para suprimir a exibição do log.		SwitchParameter
`Quiet`	Suprimir o registro em log no console.		SwitchParameter

Retorno:

- Cria um relatório que contém membros encontrados para o componente especificado.

Cmdlets de ativação do site

Para obter mais informações sobre a ativação de sites e o uso desses cmdlets, consulte Ativação de sites.

- `Set-CvadAcSiteActiveStateOnPrem` - Define o estado do site local como ativo ou inativo.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`SiteActive`	Quando presente, define o site local como ativo removendo o modo de manutenção de todos os grupos de entrega. Quando esse parâmetro não está presente, o modo de manutenção é definido em todos os grupos de entrega.		SwitchParameter
`IncludeByName`	Uma lista que especifica os nomes dos grupos de entrega que devem ser incluídos ao definir o estado ativo do site como ativo. Os caracteres curinga '*' e '?' são suportados em nomes.		Lista de cadeias de caracteres
`ExcludeByName`	Uma lista que especifica os nomes dos grupos de entrega que devem ser excluídos ao definir o estado ativo do site como ativo. Os caracteres curinga '*' e '?' são		Lista de cadeias de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	suportados em nomes.		
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false` para suprimir a exibição do log.		`$true or $false`

Retorna:

- Consulte Valores de retorno do cmdlet

- `Set-CvadAcSiteActiveStateCloud` - Define o estado do site da nuvem como ativo ou inativo.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
Parâmetros de acesso à nuvem	Consulte Parâmetros de acesso à nuvem		SwitchParameters
`SiteActive`	Quando presente, define o site na nuvem como ativo removendo o modo de manutenção de todos os grupos de entrega. Quando esse parâmetro não está presente, o modo de manutenção é definido em todos		SwitchParameter

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	os grupos de entrega.		
`IncludeByName`	Uma lista que especifica os nomes dos grupos de entrega que devem ser incluídos ao definir o estado ativo do site como ativo. Os caracteres curinga '*' e '?' são suportados em nomes.		Lista de cadeias de caracteres
`ExcludeByName`	Uma lista que especifica os nomes dos grupos de entrega que devem ser excluídos ao definir o estado ativo do site como ativo. Os caracteres curinga '*' e '?' são suportados em nomes.		Lista de cadeias de caracteres
`Quiet`	Suprimir o registro em log no console.		SwitchParameter
`DisplayLog`	Exibe o arquivo de log quando o cmdlet é concluído. Defina como `$false` para suprimir a exibição do log.		`$true or $false`

Retorna:

- Consulte Valores de retorno do cmdlet

Mesclagem de vários cmdlets de sites locais

Para obter mais informações sobre a mesclagem de sites e o uso desses cmdlets, consulte Mesclar vários sites em um único site.

- `New-CvadAcSiteMergingInfo` - Cria um conjunto de informações de prefixo/sufixo de mesclagem de sites. Não é necessário conhecer todos os prefixos ou sufixos no início. Eles podem ser atualizados com `Set-CvadAcSiteMergingInfo` ou editando manualmente o arquivo SiteMerging.yml. Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`SiteName`	O nome usado para identificar o conjunto de prefixos/sufixos para um site específico. Ele pode corresponder ao nome do site real, mas não obrigatoriamente.	x	Cadeia de caracteres
Parâmetros de fusão do site	Consulte Parâmetros de fusão do site		SwitchParameters
`Quiet`	Suprimir o registro em log no console.		SwitchParameter

  Retorna:

  - Nenhuma

- `Set-CvadAcSiteMergingInfo` - Atualiza um conjunto de informações de prefixo/sufixo de mesclagem de sites existente.

  Parâmetros:

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
`SiteName`	O nome usado para identificar o	x	Cadeia de caracteres

NOME	DESCRIÇÃO	OBRIGATÓRIO?	TIPO
	conjunto de prefixos/sufixos para um site específico. Ele pode corresponder ao nome do site real, mas não obrigatoriamente.		
Parâmetros de fusão do site	Consulte Parâmetros de fusão do site		SwitchParameters
`Quiet`	Suprimir o registro em log no console.		SwitchParameter

Retorna:

- Nenhuma

- `Remove-CvadAcSiteMergingInfo` - Remove um conjunto de informações de prefixo/sufixo de mesclagem de site existente.

  Parâmetros:

  - `SiteName` – identifica o conjunto de prefixos e sufixos do site. Esta é uma cadeia de caracteres e é obrigatória.

  Retorna:

  - Nenhuma

Parâmetros de fusão do site

Os parâmetros a seguir podem ser usados ao executar os cmdlets de mesclagem de sites. Todos os parâmetros listados são cadeias de caracteres.

- `SiteName` - o nome usado para identificar o conjunto de prefixos/sufixos para um site específico. Ele pode corresponder ao nome do site real, mas não obrigatoriamente. SiteName é um parâmetro obrigatório.
- `AdminScopedPrefix` - o prefixo que deve ser aplicado aos escopos do administrador.

- `ApplicationPrefix` - o prefixo que deve ser aplicado aos aplicativos.
- `ApplicationFolderPrefix` - o prefixo que deve ser aplicado às pastas de aplicativos; `ApplicationFolderPrefix` pode ser combinado com `ApplicationFolderRoot`.
- `ApplicationFolderRoot` - a nova pasta raiz para as pastas do aplicativo. Isso cria uma hierarquia de pastas extra. `ApplicationFolderRoot` pode ser combinado com `ApplicationFolderPrefix`.
- `ApplicationGroupPrefix` - o prefixo para grupos de aplicativos.
- `ApplicationUserPrefix` - o prefixo que deve ser aplicado ao nome do aplicativo que o usuário vê.
- `ApplicationAdminPrefix` - o prefixo que deve ser aplicado ao nome do aplicativo que o administrador vê.
- `DeliveryGroupPrefix` - o prefixo que deve ser aplicado aos grupos de entrega.
- `GroupPolicyPrefix` - o prefixo que deve ser aplicado aos nomes das políticas.
- `HostConnectionPrefix` - o prefixo que deve ser aplicado às conexões de host.
- `MachineCatalogPrefix` - o prefixo que deve ser aplicado aos catálogos de máquinas.
- `StoreFrontPrefix` - o prefixo que deve ser aplicado aos nomes do StoreFront.
- `TagPrefix` - o prefixo que deve ser aplicado às tags.
- `AdminScopedSuffix` - o sufixo que deve ser aplicado aos escopos do administrador.
- `ApplicationSuffix` - o sufixo que deve ser aplicado aos aplicativos.
- `ApplicationFolderSuffix` - o sufixo que deve ser aplicado às pastas de aplicativos; `ApplicationFolderSuffix` pode ser combinado com `ApplicationFolderRoot`.
- `ApplicationGroupSuffix` - o sufixo para grupos de aplicativos.
- `ApplicationUserSuffix` - o sufixo que deve ser aplicado ao nome do aplicativo que o usuário vê.
- `ApplicationAdminSuffix` - o sufixo que deve ser aplicado ao nome do aplicativo que o administrador vê.
- `DeliveryGroupSuffix` - o sufixo que deve ser aplicado aos grupos de entrega.
- `GroupPolicySuffix` - o sufixo que deve ser aplicado aos nomes das políticas.
- `HostConnectionSuffix` - o sufixo que deve ser aplicado às conexões do host.
- `MachineCatalogSuffix` - o sufixo que deve ser aplicado aos catálogos de máquinas.
- `StoreFrontSuffix` - o sufixo que deve ser aplicado aos nomes do StoreFront.

- `TagSuffix` - o sufixo que deve ser aplicado às tags.
- `SiteRootFolder` - o nome da pasta totalmente qualificado que deve ser usado para exportações e importações; pode ser uma pasta local ou um compartilhamento de arquivos.

Parâmetros genéricos

Parâmetros de acesso à nuvem

Todos os cmdlets que acessam a nuvem oferecem suporte aos seguintes parâmetros extras.

> **Nota:**
>
> O CustomerID, ClientID e Secret podem ser colocados no arquivo CustomerInfo.yml ou especificados com o cmdlet usando os seguintes parâmetros. Quando eles são especificados em ambos os lugares, os parâmetros do cmdlet têm precedência.

- `CustomerId` – O ID do cliente usado nas APIs Rest e é necessário para acessar todas as APIs Rest. Seu ID de cliente é encontrado no Citrix Cloud.
- `ClientId` – O ClientID criado no site Citrix Cloud Identity and Access Management. Isso é necessário para obter o token de portador necessário para autenticação de todas as APIs Rest.
- `Secret` – A chave secreta criada no site Citrix Cloud Identity and Access Management. Isso é necessário para obter o token de portador necessário para autenticação de todas as APIs Rest.
- `CustomerInfoFileSpec` — A especificação do arquivo que aponta para um arquivo de informações do consumidor para substituir o local e o nome padrão.

Parâmetros do modo de migração

Os cmdlets que modificam a configuração do site na nuvem (`Import`, `Restore`, `Merge`, `New` e `Sync`) oferecem suporte aos seguintes parâmetros extras para fornecer mais flexibilidade.

- `CheckMode` – Executa a operação de importação, mas *não* faz alterações. Todas as alterações esperadas são relatadas antes da conclusão da importação. Você pode usar esse comando para testar sua importação antes que ela ocorra.
- `BackupFirst` – Faz backup do conteúdo da nuvem em arquivos .yml antes de modificar a configuração da nuvem. Essa opção está ativada por padrão.

- `Confirm` – Quando true, solicita que os usuários confirmem que desejam fazer alterações na configuração do site na nuvem. O cmdlet `Remove` mostra um prompt devido à sua natureza destrutiva. Defina como false se não desejar nenhum prompt, como executar dentro de scripts automatizados. O padrão de `Confirm` é true.
- `SecurityFileFolder` – Esta é a pasta totalmente qualificada que contém o arquivo CustomerInfo.yml que pode apontar para uma pasta local ou uma pasta de compartilhamento de rede que pode estar sob controle de autenticação. A ferramenta não solicitará credenciais; o acesso ao recurso controlado deve ser obtido antes de executar a ferramenta.
- `SiteName` – Especifica o prefixo de mesclagem do site e o sufixo definidos a serem usados ao importar.
- `SiteActive` – Especifica se o site importado está ativo ou inativo. Por padrão, esse parâmetro é definido como `$false`, o que significa que o site importado está inativo.

Parâmetros de exibição de log

Os cmdlets `Export`, `Import`, `Sync`, `Restore`, `Backup`, `Compare` e `Remove` exibem o arquivo de log quando a operação é concluída. Você pode suprimir a exibição definindo o parâmetro `-DisplayLog` como `$false`. O Notepad.exe é usado como padrão para exibir o arquivo de log. Você pode especificar um editor diferente no arquivo CustomerInfo.yml.

`Editor: C:\Program Files\Notepad++\notepad++.exe`

Valores de retorno do cmdlet

ActionResult

Todos os cmdlets retornam o seguinte valor.

```
public class ActionResult

{

    public bool                         Overall_Success;

    public Dictionary&lt;string, string>   Individual_Success;

    public object                       CustomResult;

}
```

`Overall_Success` retorna um único booleano que mostra o sucesso geral do cmdlet em todos os componentes selecionados: verdadeiro, que significa bem-sucedido, e falso, que significa malsucedido.

`Individual_Success` retorna um ou três valores para cada componente principal. O resultado de um componente pode ser Success, Failure ou Skipped. Skipped indica que o componente não foi selecionado para execução pelo cmdlet.

`CustomResult` é específico do cmdlet.

CustomResult

`Import`, `Merge`, `Restore`, `Sync`, `Compare`, `Compare File` e `Remove` retornam as seguintes informações de resultados personalizados para uma única instância do `EvaluationResultData`.

> **Nota:**
>
> Os cmdlets `Export` e `Template` não retornam um resultado personalizado.

```
 public class EvaluationResultData

 {

     public Dictionary<string, Dictionary&lt;string, ActionResultValues >>
EvaluationResults;

     public int                  Added;

     public int                  Updated;

     public int                  Deleted;

     public int                  NoChange;

     public int                  TotalChanged;

     public EvaluationResults     OverallResult;

     public string               CloudBackupFolder;
```

```
    public string               SourceBackupFolder;

 }

 Where:

 public enum ActionResultValues

{

    Add,

    Update,

    Delete,

    Identical,

    DoNothing

 }

 public enum EvaluationResults

 {

    Success,

    Failure,

    Skipped

 }
```

`EvaluationResults` exibe uma lista com uma entrada por componente selecionado. A chave é o nome do componente e o valor é uma lista de cada membro do componente e a ação executada nesse membro do componente. As ações podem ser qualquer um dos valores de `ActionResultValues`.

`Added`, `Updated`, `Deleted`, e `NoChange` indicar que o número total de membros do componente adicionados, atualizados, excluídos ou nenhuma ação executada, nessa ordem.

`TotalChanged` é a soma de `Added`, `Updated` e `Deleted`.

`OverallResult` é um único booleano que indica o resultado do cmdlet. O valor true indica sucesso total em todos os componentes e false indica falha no processamento de um ou mais componentes.

`CloudBackupFolder` é a especificação de arquivo totalmente qualificada do backup de configuração do site na nuvem antes do cmdlet executar qualquer ação de modificação na nuvem.

`SourceBackupFolder` é a especificação de arquivo totalmente qualificada do backup do arquivo de origem feito após a conclusão do cmdlet. Por padrão, esses arquivos estão em *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Ajuda do PowerShell

A ajuda do PowerShell está disponível para cada cmdlet. Todos os parâmetros são documentados com cada cmdlet, juntamente com uma breve explicação sobre o cmdlet. Para acessar a ajuda de qualquer cmdlet, digite `Get-Help` na frente do cmdlet.

```
Get-Help Import-CvadAcToSite
```

Solucionar problemas de configuração automatizada e informações adicionais

> **Importante:**

> Para ver as mensagens de erro que ocorrem com frequência para a Configuração automatizada e as soluções correspondentes, consulte *troubleshooting FAQ* no artigo do Centro de Conhecimento CTX277730.

Erros da ferramenta Automated configuration

Às vezes, as operações da ferramenta Automated configuration podem produzir erros. Quando isso acontece, podem ocorrer falhas ao processar componentes como catálogos de máquinas, grupos de entrega ou políticas de grupo, por exemplo. O uso de `OnErrorAction` e parâmetros de continuação permitem que você detecte erros durante o processamento, resolva-os e continue de onde parou.

O valor padrão `OnErrorAction` é `StopCompEnd`. Quando ocorre um erro, a ferramenta termina de processar o componente atual. Nenhum componente adicional é processado e os erros não

são transferidos para os componentes dependentes posteriores. Depois de resolver os erros, você pode executar novamente seus cmdlets com qualquer parâmetro de continuação aplicado.

Parâmetro OnErrorAction

Você pode definir valores do parâmetro `OnErrorAction` nos cmdlets de migração para controlar como a ferramenta responde aos erros encontrados ao processar componentes.

Esta tabela mostra os valores dos parâmetros e suas descrições:

VALOR	DESCRIÇÃO
`Continue`	Tenta processar o máximo possível de todos os componentes.
`Pause`	Pausa no final do processamento e solicita que você continue ou pare.
`StopCompEnd`	Tenta processar o máximo possível do componente. Para após a conclusão do componente. (Padrão)

Cmdlets de migração

Você pode aplicar o parâmetro `OnErrorAction` aos seguintes cmdlets de migração:

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

Exemplo: `Merge-CvadAcToSite -OnErrorAction StopImmediately`

Parâmetros Resume

Esses parâmetros definem como a ferramenta é retomada após uma pausa ou interrupção da operação devido a um erro.

Você pode aplicar parâmetros Resume aos cmdlets de migração que incluam um dos seguintes valores de parâmetro `OnErrorAction`:

- `Pause`

- `StopCompEnd`
- `StopImmediately`

Esta tabela mostra os valores dos parâmetros e suas descrições:

VALOR	DESCRIÇÃO
`-AllRemaining`	Requer um componente inicial. O processamento começa no componente inicial e processa todos os componentes restantes. Vários componentes são processados.
`-Resume`	Usa o componente do CurrentComponent.txt como ponto de partida. All Remaining é definido como true. Vários componentes são processados.
`-Repeat`	Usa o componente do CurrentComponent.txt como ponto de partida. All Remaining é definido como false. Somente um componente é processado.

O último componente processado é armazenado no arquivo CurrentComponent.txt na pasta AutoConfig. Não é recomendado editar esse arquivo. Se você especificar `-Resume` ou `-Repeat` e CurrentComponent.txt estiver ausente ou for inválido, o processamento será interrompido e você será solicitado a selecionar um componente.

Configurando o OnErrorAction no arquivo CustomerInfo.yml

Você também pode definir valores `OnErrorAction` no arquivo CustomerInfo.yml. Defina os valores usando os seguintes cmdlets:

- Para um novo arquivo: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- Para um arquivo existente: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

Logs

A execução de qualquer cmdlet resulta na criação de um arquivo de log e em uma entrada no arquivo de log do histórico principal. Todos os arquivos de log de operação são colocados em uma pasta de backup. Todos os nomes de arquivos de log começam com `CitrixLog` e mostram a

operação de configuração automática e a data e o carimbo de data/hora da execução do cmdlet. Os logs não são excluídos automaticamente.

O registro do histórico principal está localizado em *%HOMEPATH%\Documents\Citrix\AutoConfig*, no arquivo chamado **History.Log**. Cada execução de cmdlet resulta em uma entrada de log principal contendo a data, a operação, o resultado, o backup e os locais do arquivo de log da execução.

Você também pode usar o cmdlet `New-CvadAcZipInfoForSupport` para coletar logs que devem ser enviados à Citrix para suporte. Esse cmdlet compacta todos os arquivos de log e .yml em um único arquivo zip. Informações confidenciais do consumidor (CustomerInfo.yml e CvadAcSecurity.yml) não estão incluídas no zip. O arquivo Icon.yml também é excluído devido ao seu tamanho. O arquivo zip é colocado em *%HOMEPATH%\Documents\Citrix\AutoConfig* e nomeado *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, com base na data e no carimbo de data/hora. Esse arquivo zip também pode funcionar como um backup.

Cada arquivo de log inclui o seguinte:

- O nome da operação e se o modo de verificação está ativado
- A data e a hora de início e término
- Várias entradas para as ações de cada componente e notificações de sucesso/falha
- Resumo das ações realizadas, incluindo várias contagens de objetos criados
- Correções sugeridas, quando aplicável
- Local da pasta de backup, quando aplicável
- Local do registro principal
- Duração

Arquivos de diagnóstico

Os arquivos de diagnóstico ajudam você a determinar e resolver problemas. Os arquivos a seguir são criados quando a operação é executada. Eles estão localizados na subpasta específica da ação em *%HOMEPATH%\Documents\Citrix\AutoConfig*. Inclua esses arquivos ao fornecer informações para suporte à resolução de problemas.

Exportar

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

Esse arquivo conta todas as chamadas do Broker PowerShell SDK feitas para exportar a configuração do site para arquivos.

Importar, mesclar, restaurar, sincronizar, fazer backup, comparar

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

Esse arquivo documenta cada chamada da API Rest e as informações relacionadas.

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

Esse arquivo contém todo o conteúdo da API Rest `Add`, `Update` e `Delete`.

Problemas resultantes de dependências

Importações e mesclagens podem falhar devido à falta de dependências. Alguns problemas comuns são:

1. As Políticas de Grupo não têm filtros de grupo de entrega. As causas usuais são grupos de entrega que não foram importados.
2. Os aplicativos não conseguem importar ou mesclar. A causa usual é a falta de grupos de entrega ou grupos de aplicativos que não foram importados.
3. Os grupos de aplicativos não têm um RestrictToTag. As causas usuais são tags que não foram importadas.
4. As conexões do host falham. A causa usual é falta de informações de segurança no arquivo CvadAcSecurity.yml.
5. Os catálogos de máquinas falham. A causa usual são as conexões de host que não foram importadas.
6. Máquinas ausentes em catálogos de máquinas e grupos de entrega. A causa usual são máquinas que não foram encontradas no Active Directory.
7. Usuários ausentes nos grupos de entrega. A causa comum são os usuários que não foram encontrados no Active Directory.

Recomendações, em Recommendations

- Não execute mais de uma instância de Automated configuration por vez. A execução de várias instâncias simultâneas produz resultados imprevisíveis no site da nuvem. Se isso ocorrer, execute novamente uma instância de Automated configuration para trazer o site para o estado esperado.
- Não trabalhe nem altere dados na guia Manage em Full Configuration ao executar a Automated configuration.
- Sempre verifique visualmente os resultados de mesclagem/importação/restauração em Full Configuration para garantir que o site da nuvem atenda às expectativas.

Pastas

Local de raiz da pasta padrão

Todas as operações da ferramenta Automated configuration ocorrem na pasta raiz ou em subpastas dentro dela. A pasta raiz está localizada em *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Exportar

Todos os arquivos exportados são colocados em dois locais de pasta, proporcionando facilidade de uso e um histórico de exportações. As exportações são sempre colocadas na pasta raiz. As cópias são colocadas em uma subpasta chamada **Exportar** com a data e a hora da exportação.

A pasta raiz sempre contém a configuração de site local exportada mais recente. Cada subpasta **Export** contém a exportação feita na data e hora indicadas, o que mantém um histórico de exportações. Você pode usar qualquer subpasta **Export** para configurar o site da nuvem. A configuração automatizada não exclui nem modifica subpastas de exportação existentes.

Importar/Mesclar/Sincronizar/Comparar

As operações `Import`, `Merge` e `Compare` sempre são originadas de arquivos localizados na pasta raiz. Cada operação resulta na criação de uma subpasta para a qual os arquivos na pasta raiz são copiados, fornecendo um histórico de alteração dos arquivos de origem do site na nuvem.

Restaurar

A operação `Restore` usa uma subpasta existente para configurar o site da nuvem. A pasta de origem é especificada no parâmetro `-RestoreFolder` necessário. Ao contrário de outros comandos, nenhuma nova subpasta é criada porque a operação `Restore` usa uma subpasta existente. A pasta de restauração pode ser a pasta raiz, mas ainda deve ser especificada no parâmetro `-RestoreFolder` .

Backups

A Configuração automatizada inicializa, atualiza e faz backup de uma configuração de site na nuvem. Quando usadas ao longo do tempo, muitas configurações diferentes podem mudar no site da nuvem. Para facilitar o uso a longo prazo e preservar as alterações do histórico, a Configuração Automatizada usa um esquema de preservação para salvar esse histórico de alterações e fornecer um método para restaurar estados anteriores.

Os backups de configuração do site em nuvem são sempre feitos em uma subpasta chamada **Backup** com os dados e a hora do backup. A Configuração Automatizada não exclui nem modifica subpastas de exportação existentes.

Você pode usar os backups para restaurar componentes específicos ou toda a configuração. Para restaurar todo o grupo de entrega e os componentes do catálogo de máquinas, use o cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **Nota:**
>
> As informações do arquivo de backup no cmdlet anterior são baseadas em seus próprios backups.

Para restaurar toda a configuração do site de nuvem, use o cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss
```

> **Nota:**
>
> As informações do arquivo de backup no cmdlet anterior são baseadas em seus próprios backups.

Alteração da pasta raiz padrão

As operações `Export`, `Import`, `Merge`, `Sync` e `Compare` podem alterar a pasta raiz padrão por meio do parâmetro `–AlternateFolder`. A criação e o gerenciamento de subpastas por operação permanecem os mesmos descritos anteriormente.

Arquivos copiados para subpastas

Todos os arquivos com uma extensão ".yml" são copiados para as subpastas de operação, exceto o seguinte:

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

Backups automatizados de sites em nuvem à prova de falhas

Um backup da configuração atual do site na nuvem é feito antes de executar operações que alteram a configuração. Isso inclui os parâmetros `Import`, `Merge`, `Sync` e `Restore`. O backup está sempre em uma subpasta abaixo da subpasta operacional.

No caso de `Restore`, a pasta de backup é uma subpasta da pasta especificada no parâmetro `-RestoreFolder`.

Automação

Os cmdlets da ferramenta Automated configuration podem ser executados em scripts de automação sem a intervenção do administrador, suprimindo os prompts e a exibição dos resultados do log na conclusão do cmdlet. Você também pode definir parâmetros para fazer o mesmo usando o arquivo CustomerInfo.yml.

Adicione o parâmetro a seguir aos cmdlets de modificação da nuvem para suprimir a exibição de prompts.

`-Confirm $false`

Adicione o seguinte parâmetro aos cmdlets para suprimir a exibição do log na conclusão do cmdlet.

`-DisplayLog $false`

Adicione o seguinte parâmetro aos cmdlets para suprimir o registro na janela de comando do PowerShell.

`-Quiet`

Como outro método, os seguintes parâmetros podem ser colocados no arquivo CustomerInfo.yml.

`Confirm: False`

`DisplayLog: False`

Exportar de PCs que não sejam o Delivery Controller

A ferramenta Automated configuration usa vários SDKs do Citrix PowerShell para exportar a configuração do site local para arquivos. Esses SDKs são instalados automaticamente no Delivery Controller, permitindo que a ferramenta seja executada no Delivery Controller sem ações extras. Ao executar em máquinas que não são Delivery Controller, é necessário instalar o conjunto de SDKs do Citrix PowerShell necessários para a ferramenta. Esse conjunto de SDK faz parte do

Citrix Studio, que pode ser instalado a partir da mídia de instalação do Citrix Virtual Apps and Desktops.

> **Nota:**
>
> A configuração automatizada não pode ser executada no Cloud Connector.

Mudança para o Citrix Cloud Government e o Japan Control Plane

Os ambientes Citrix Cloud Government e Japan Control Plane usam diferentes pontos de acesso para autenticar e alocar tokens de acesso. Esse requisito exclusivo se aplica a qualquer ferramenta Automated configuration que acesse a nuvem. Execute as etapas a seguir para usar a Configuração automatizada nesses ambientes.

1. Na pasta *%HOMEPATH%\Documents\Citrix\AutoConfig*, edite CustomerInfo.yml.
2. Adicione uma das seguintes linhas, dependendo do ambiente ao qual você deseja se conectar, a CustomerInfo.yml (ou altere-a, se já estiver presente).

   ```
   Environment: 'ProductionGov'
   ```

   ou

   ```
   Environment: 'ProductionJP'
   ```

A Configuração Automatizada agora pode ser usada nesses ambientes.

Coleta de dados do Citrix Cloud

Para obter informações sobre quais informações o Citrix Cloud coleta, consulte Citrix Cloud Services Customer Content and Log Handling.

Recursos adicionais

Fórum de discussão

Visite o Citrix Discussion forum for Automated Configuration.

Vídeo

Assista Under the Hood of the Automated Configuration Tool for Citrix Virtual Apps and Desktops no YouTube.

Treinamento

O Cloud Learning Center contém guias de vídeo passo a passo para criar uma implantação de serviço, incluindo as tarefas descritas neste artigo. Consulte Migrating Citrix Virtual Apps and Desktops to Citrix Cloud Learning Path.

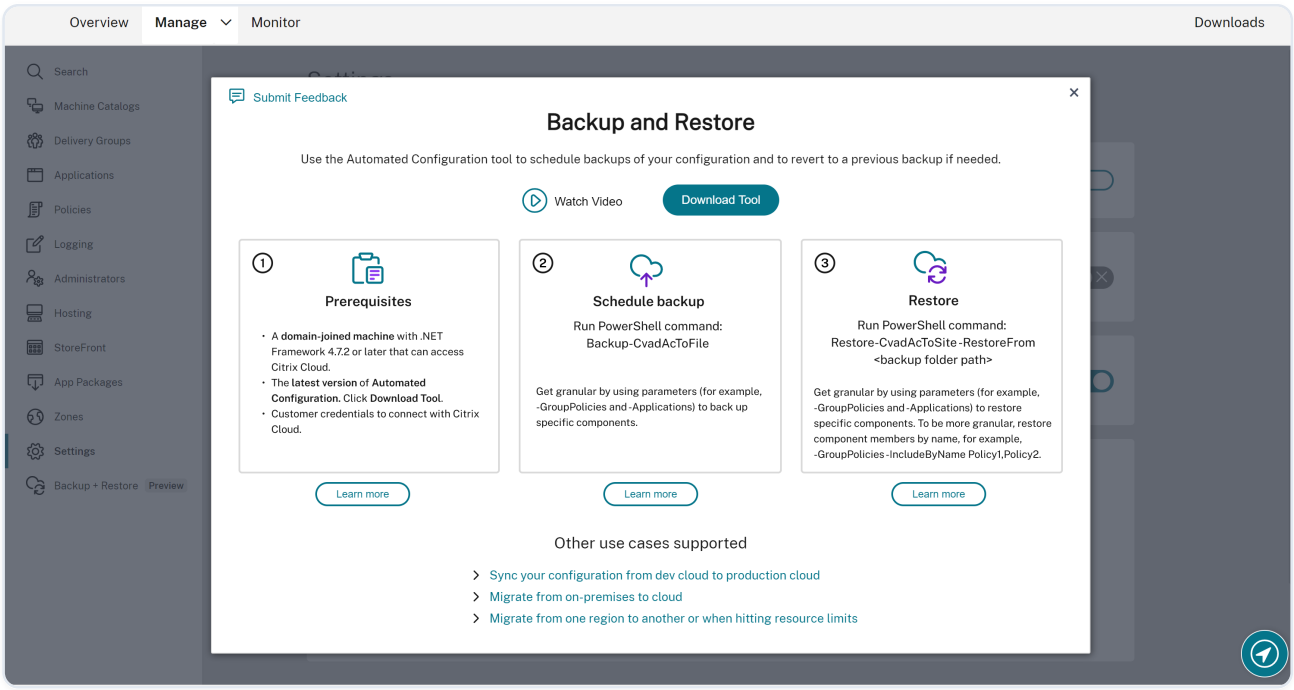
Migração da nuvem para a nuvem

A Configuração Automatizada permite automatizar a migração de sua configuração de nuvem para outro site de nuvem ou permitir que você restaure seu próprio site de nuvem.

Usar a Configuração Automatizada pode resolver muitos casos de uso:

- Sincronizar seu site do teste ou do estágio para a produção
- Fazer Backup e restauração da sua configuração
- Atingir limites de recursos
- Migrar de uma região para outra

Em Full Configuration no Citrix Cloud, consulte o nó Backup e restauração para obter informações sobre a Configuração automatizada e como ela pode ser usada para migrar sua configuração da nuvem para a nuvem.



Pré-requisitos para migrar sua configuração

Para fazer backup e restaurar sua configuração, você precisa:

- Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) provisionado.

- Um local de recurso ativo com o Connector instalado.
- A conectividade com sites que acessam o Citrix Cloud deve ser permitida e estar disponível. Para obter mais informações, consulte Requisitos de sistema e conectividade.

> **Nota:**
>
> Não é possível fazer backup do MCS da nuvem usando a Configuração Automatizada.

Backup da configuração do Citrix DaaS

> **Importante:**
>
> - Você deve ter o arquivo CustomerInfo.yml com o ID do consumidor, o ID do cliente e as informações da chave secreta incluídas. Para obter mais informações sobre como recuperar o ID do cliente, o ID do consumidor e a chave secreta, consulte Geração do ID do consumidor, o ID do cliente e a chave secreta. Para obter informações sobre como adicionar essas informações ao arquivo CustomerInfo.yml, consulte Preenchendo o arquivo de informações do cliente.
> - O arquivo ZoneMapping.yml deve incluir informações que mapeiam os locais dos recursos na nuvem. Para obter mais informações sobre como mapear suas zonas, consulte Preenchimento do arquivo de mapeamento de zona.
> - Se você tiver conexões de host, deverá inserir as informações correspondentes no arquivo CvadAcSecurity.yml.

1. Instalar a Configuração Automatizada.

   > **Nota:**
   >
   > Para a migração de nuvem para nuvem, a Configuração Automatizada pode ser instalada em uma máquina com acesso à Internet à qual o administrador tenha acesso direto.

2. Clique duas vezes no ícone **Configuração Automatizada**. Uma janela do PowerShell é exibida.
3. Execute o seguinte comando para fazer um backup.

   ```
   Backup-CvadAcToFile
   ```

Depois de executar qualquer cmdlet pela primeira vez, é criada uma pasta de exportação com os arquivos de configuração .yml e logs. A pasta está em *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Se você encontrar erros ou exceções, consulte a seção **Correções** no arquivo de log.

Restaurar sua configuração para o Citrix DaaS

1. Clique duas vezes no ícone **Configuração Automatizada**. Uma janela do PowerShell é exibida.
2. Execute o seguinte comando para fazer uma restauração.

   ```
   Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
   ```

Verifique o estado esperado com o novo estado atual.

Depois de executar o cmdlet, é criada uma pasta de exportação com os arquivos de configuração .yml e logs. A pasta está em *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Se você encontrar erros ou exceções, consulte a seção **Correções** no arquivo de log.

O processo de backup e restauração protege você contra alterações não intencionais na configuração do site na nuvem ou corrompimento. Embora a Configuração Automatizada faça backups sempre que é feita uma alteração, esse backup reflete o estado da configuração do site na nuvem antes das alterações. Proteger-se exige que você faça backup periódico da configuração do site na nuvem e salve em um local seguro. Se ocorrer uma alteração ou corrompimento indesejável, o backup poderá ser usado para corrigir a alteração ou corrupção em um nível de configuração de site granular ou completo.

Migração granular

> **Importante:**

> Para obter mais informações sobre a ordem de migração de componentes, consulte Ordem de migração de componentes.

Restaurando componentes inteiros

A restauração de um componente envolve a seleção de um ou mais parâmetros de componentes.

Para restaurar todo o grupo de entrega e os componentes do catálogo de máquinas, siga este exemplo:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss
```

Restaurando membros do componente

A restauração de um ou mais membros do componente faz uso do recurso `IncludeByName`. O cmdlet `Restore` é chamado com o parâmetro `RestoreFolder` junto com o componente único selecionado e a lista de inclusão.

Para restaurar duas políticas de grupo de um backup, siga este exemplo:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss
```

```
-GroupPolicies -IncludeByName Policy1,Policy2
```

```
-DeliveryGroups -MachineCatalogs
```

Restaurando toda a configuração do site na nuvem

Restaurar a configuração completa do site na nuvem significa selecionar todos os componentes para restaurar.

Para restaurar toda a configuração do site na nuvem, siga este exemplo:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss
```

Ativação de sites

A ativação do site permite que você controle qual site está ativo e controla seus recursos. Para obter mais informações, consulte Ativação de sites.

Migração do local para a nuvem

A Configuração Automatizada permite automatizar a movimentação da configuração local para um site na nuvem.

A imagem a seguir é uma visão de alto nível do que a Configuração Automatizada pode fazer para migrar sua configuração para a nuvem.



Pré-requisitos para migrar sua configuração

Para *exportar* sua configuração do Citrix Virtual Apps and Desktops, você precisa:

- Citrix Virtual Apps and Desktops: versão atual e seu antecessor imediato ou Citrix Virtual Apps and Desktops, XenApp e XenDesktop LTSRs: todas as versões
- Uma máquina ingressada no domínio com .NET Framework 4.7.2 ou posterior e o Citrix PowerShell SDK. Isso é instalado automaticamente no Delivery Controller. (Para ser executado em uma máquina que não seja o Delivery Controller local, o Citrix Studio deve ser instalado, pois o Studio instala os snap-ins corretos do PowerShell. O instalador do Studio pode ser encontrado na mídia de instalação do Citrix Virtual Apps and Desktops.)

Para *importar* sua configuração para o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), você precisa:

- Uma máquina com acesso ao Citrix Cloud. Isso não precisa ser um Delivery Controller ou uma máquina ingressada no domínio.
- Citrix DaaS provisionado.
- Um local de recurso ativo com o Connector instalado e ingressado no mesmo domínio da configuração local.
- A conectividade com sites que acessam o Citrix Cloud deve ser permitida e estar disponível. Para obter mais informações, consulte Requisitos de sistema e conectividade.

> **Nota:**

> A Configuração automatizada não pode ser instalada em um sistema do Cloud Connector. Se estiver executando a Configuração Automatizada em um servidor que não seja o Delivery Controller, você deverá usar o parâmetro -AdminAddress e especificar o nome DNS ou o endereço IP do Delivery Controller. Por exemplo, `Export-CvadAcToFile -AdminAddress 192.168.0.10`

Exportando sua configuração local do Citrix Virtual Apps and Desktops

Importante:

- Você deve ter o arquivo CustomerInfo.yml com o ID do consumidor, o ID do cliente e as informações da chave secreta incluídas. Para obter mais informações sobre como recuperar o ID do cliente, o ID do consumidor e a chave secreta, consulte Geração do ID do consumidor, o ID do cliente e a chave secreta. Para obter informações sobre como adicionar essas informações ao arquivo CustomerInfo.yml, consulte Preenchendo o arquivo de informações do cliente.
- O arquivo ZoneMapping.yml deve incluir informações que mapeiam sua zona local para locais de recursos na nuvem. Para obter mais informações sobre como mapear suas zonas, consulte Preenchimento do arquivo de mapeamento de zona.
- Se você tiver conexões de host, deverá inserir as informações correspondentes no arquivo CvadAcSecurity.yml.

1. Instalar a Configuração Automatizada.
2. Clique duas vezes no ícone **Configuração Automatizada**. Uma janela do PowerShell é exibida.
3. Execute o seguinte comando para exportar todos os componentes. Exportar sua configuração local *não* a altera de forma alguma.

   ```
   Export-CvadAcToFile
   ```

Depois de executar qualquer cmdlet pela primeira vez, é criada uma pasta de exportação com os arquivos de configuração .yml e logs. A pasta está em *%HOMEPATH%\Documents\Citrix\AutoConfig*. Cada exportação sucessiva cria uma subpasta. A pasta pai *%HOMEPATH%\Documents\Citrix\AutoConfig* sempre contém os arquivos exportados da exportação mais recente.

Nota:

Se a Configuração Automatizada não estiver instalada no Delivery Controller, execute `import-module Citrix.AutoConfig.Commands` antes de usar a ferramenta por meio do PowerShell. Essa etapa não será necessária se você abrir a Configuração automatizada usando o ícone **Configuração Automatizada**.

> Se você encontrar erros ou exceções, consulte a seção **Correções** no arquivo de log.

Importar sua configuração para o Citrix DaaS

> **Importante:**
>
> - Você deve ter o arquivo CustomerInfo.yml com o ID do consumidor, o ID do cliente e as informações da chave secreta incluídas. Para obter mais informações sobre como recuperar o ID do cliente, o ID do consumidor e a chave secreta, consulte Geração do ID do consumidor, o ID do cliente e a chave secreta. Para obter informações sobre como adicionar essas informações ao arquivo CustomerInfo.yml, consulte Preenchendo o arquivo de informações do cliente.
> - O arquivo ZoneMapping.yml deve incluir informações que mapeiam sua zona local para locais de recursos na nuvem. Para obter mais informações sobre como mapear suas zonas, consulte Preenchimento do arquivo de mapeamento de zona.
> - Se você tiver conexões de host, deverá inserir as informações correspondentes no arquivo CvadAcSecurity.yml.

Execução de uma importação

1. Clique duas vezes no ícone **Configuração Automatizada**. Uma janela do PowerShell é exibida.
2. Execute o seguinte comando para importar todos os componentes.

   ```
   Merge-CvadAcToSite
   ```

Verifique o estado esperado com o novo estado atual. Várias opções de importação controlam se os resultados da importação são idênticos ou um subconjunto do site local.

Depois de executar o cmdlet, é criada uma pasta de exportação com os arquivos de configuração .yml e logs. A pasta está em *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Se você encontrar erros ou exceções, consulte a seção **Correções** no arquivo de log.

> **Nota:**

> Se a Configuração Automatizada não estiver instalada no Delivery Controller, execute `import-module Citrix.AutoConfig.Commands` antes de usar a ferramenta por meio do PowerShell. Essa etapa não será necessária se você abrir a Configuração automatizada usando o ícone **Configuração Automatizada**.

> Para reverter para a configuração original do Citrix DaaS, consulte Backup da configuração do Citrix DaaS.

Operação de importação em detalhes

O processo de importação foi concebido para executar atualizações com precisão, executar apenas as atualizações necessárias e verificar se todas as atualizações foram feitas corretamente. As etapas seguidas em todas as operações de importação estão descritas abaixo.

1. Ler o arquivo .yml exportado (estado esperado).
2. Ler a nuvem (estado atual).
3. Fazer backup do estado da nuvem de pré-importação para arquivos .yml (o pré-backup pode ser restaurado, se necessário).
4. Avaliar as diferenças entre o estado esperado e o atual. Isso determina quais atualizações devem ser feitas.
5. Fazer as atualizações.
6. Ler novamente a nuvem (novo estado atual).
7. Fazer backup do estado da nuvem pós-importação para arquivos .yml (o pós-backup pode ser restaurado, se necessário).
8. Comparar o novo estado atual com o estado esperado.
9. Relatar os resultados da comparação.

Migração granular

> **Importante:**

> Para obter mais informações sobre a ordem de migração de componentes, consulte Ordem de migração de componentes.

> Você pode migrar seletivamente apenas componentes ou até mesmo apenas nomes de componentes.

- Os parâmetros de componentes suportados incluem `MachineCatalogs`, `Tags` e mais.
- Parâmetros de nome de componente suportados incluem `IncludeByName` e `ExcludeByName` parâmetros e outros.

Para obter mais informações sobre parâmetros e como usá-los, consulte Parâmetros de migração granular.

Ativação de sites

A ativação do site permite que você controle qual site está ativo e controla seus recursos. Para obter mais informações, consulte Ativação de sites.

Mesclar vários sites em um único site

O suporte a vários sites para a Configuração Automatizada fornece um método para mesclar vários sites locais em um único site de nuvem.

O suporte a vários sites adiciona prefixos e sufixos exclusivos aos nomes dos componentes por site local, garantindo a exclusividade do nome depois que vários sites locais são mesclados em um único site na nuvem.

Podem ser atribuídos prefixos e sufixos a cada um dos seguintes componentes por site local.

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`
- `StoreFront`
- `Tag`

As pastas de aplicativos suportam prefixo, sufixo e rerooting. O rerooting adiciona uma pasta de nível superior extra à estrutura de pastas já existente de um aplicativo.

Regras de prefixação e sufixo

1. Os prefixos e sufixos não podem conter nenhum dos seguintes caracteres especiais:
   `\ , / ; : # . * ? = < > | ( ) " ' { } [ ]`
2. Os prefixos e sufixos podem conter espaços à direita, mas não espaços à esquerda.
3. Os prefixos e sufixos devem ter aspas duplas para conter espaços à direita.
4. Os prefixos e sufixos são aplicados no momento da importação, mesclagem e adição. Os arquivos .yml de origem nunca são modificados.
5. O processo de prefixação e sufixação automaticamente prefixa ou sufixa nomes de componentes dependentes quando aplicável. Por exemplo, se os nomes de catálogo de máquinas forem prefixados com "East", os grupos de entrega que fazem referência a eles também serão prefixados com "East".
6. Se o nome de um componente já começar com o prefixo ou o sufixo, nenhum prefixo ou sufixo será adicionado. Os nomes dos componentes não podem conter prefixos ou sufixos duplos idênticos.
7. Os prefixos e sufixos podem ser usados individualmente ou em combinação.
8. O uso de um prefixo ou sufixo em um componente é opcional.

> **Nota:**
>
> A interface Full Configuration exibe os componentes em ordem alfabética.

Agrupar por site

Use o prefixo para agrupar visualmente componentes de um único site. Cada site é listado em seu próprio grupo, com prefixo, controlando alfabeticamente a ordem de diferentes grupos de sites.

Agrupar por nome

Use o sufixo para agrupar visualmente componentes com nomes semelhantes de vários sites. Componentes com nomes semelhantes de diferentes sites alternam visualmente.

Arquivo SiteMerging.yml

O prefixo do site começa com o arquivo SiteMerging.yml que contém o prefixo do site e o mapeamento de sufixos para um ou mais sites locais. Você pode gerenciar o arquivo

SiteMerging.yml manualmente ou usando os cmdlets disponíveis listados na seção Mesclagem de vários cmdlets de sites locais .

Exportar, importar, mesclar e adicionar

A mesclagem não pode começar até que você tenha exportado um site local. Para exportar um site local, consulte Migração do local para a nuvem.

Pasta de destino de exportação central

Os métodos descritos nesta seção colocam várias exportações de sites em um local central de compartilhamento de arquivos. O arquivo SiteMerging.yml, o arquivo CustomerInfo.yml e todos os arquivos de exportação permanecem nesse local de compartilhamento de arquivos, permitindo que você faça a importação de um local independente dos sites locais.

As operações de acesso à nuvem nunca fazem referência aos sites locais ou ao Active Directory, permitindo que você faça operações de acesso à nuvem de qualquer lugar.

Compartilhamento direto de arquivos

As operações de exportação, importação, mesclagem e novo/adição fornecem um parâmetro para direcionar ou criar uma pasta diferente da pasta padrão, *%HOMEPATH%\Documents\Citrix\AutoConfig*. Os exemplos a seguir usam um compartilhamento de arquivos central localizado em `\\share.central.net`, local a que o administrador já tem acesso, tendo fornecido as credenciais conforme o necessário.

Para direcionar a exportação para uma pasta específica do site, use o parâmetro `-TargetFolder`:

Do East DDC:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\SiteEast
```

Do West DDC:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\SiteWest
```

Depois que as exportações forem concluídas, crie os arquivos CustomerInfo.yml e SiteMerging.yml e coloque-os em `\\share.central.net\AutoConfig`.

> **Nota:**

> Não use o parâmetro `SiteRootFolder` ao criar o SiteMerging.yml ao usar esse método de referência de compartilhamento de arquivo direto.

> Para importar, mesclar ou adicionar do compartilhamento direto de arquivos, você deve decidir de qual máquina deseja fazer a operação de acesso à nuvem. As opções são:

- Um dos DDCs locais em que a ferramenta já está instalada.
- A máquina que hospeda o compartilhamento de arquivos.
- Uma máquina diferente.

A Configuração Automatizada deve ser instalada na máquina que acessa a nuvem. Nem o PowerShell SDK, o DDC nem o Active Directory no local são usados, portanto, os requisitos de execução de acesso à nuvem são mais simples do que os requisitos de exportação.

Para mesclar o East DDC com a nuvem:

```
Merge-CvadAcToSite –SiteName East –SourceFolder \
\share.central.net\AutoConfig\SiteEast -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

Para mesclar o West DDC com a nuvem:

```
Merge-CvadAcToSite –SiteName West –SourceFolder \
\share.central.net\AutoConfig\SiteWest -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

Veja a seguir um exemplo de arquivo SiteMerging.yml usado no exemplo anterior.

```
East:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"
```

```
  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"

  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"

  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"
```

```
  TagSuffix: "_east"

West:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "

  AdminScopeSuffix: ""

  AdminRoleSuffix: ""

  ApplicationAdminSuffix: ""

  ApplicationFolderSuffix: ""

  ApplicationGroupSuffix: ""
```

```
ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

Referência de compartilhamento de arquivos usando SiteMerging.yml

Esse método usa o membro `SiteRootFolder` do conjunto de prefixos do site. Embora seja mais complexo do que o método de compartilhamento direto de arquivos, esse método reduz as chances de direcionar a pasta errada ao exportar, importar, mesclar ou adicionar.

Primeiro, defina o `SiteRootFolder` para cada site no arquivo SiteMerging.yml Você deve fazer isso no local compartilhado.

`New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \ \\share.central.net\AutoConfig\SiteEast -TargetFolder \ \\share.central.net\AutoConfig`

`New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest -TargetFolder \\share.central.net\AutoConfig`

Neste exemplo, East é uma especificação de pasta totalmente qualificada e West é uma especificação de pasta relativa.

Para direcionar a exportação para uma pasta específica do site usando o arquivo SiteMerging.yml:

Do East DDC:

`mkdir \\share.central.net\AutoConfig\SiteEast`

`Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \ \\share.central.net\AutoConfig\CustomerInfo.yml`

Do West DDC:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

O cmdlet de exportação usa o local da pasta CustomerInfo.yml para localizar o arquivo SiteMerging.yml. No caso do East, o `SiteRootFolder` é totalmente qualificado. Ele é usado como está. No caso de West, o não `SiteRootFolder` está totalmente qualificado. Ele é combinado com o local da pasta CustomerInfo.yml para recuperar um local de pasta totalmente qualificado para West.

Para mesclar o East DDC com a nuvem:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

Para mesclar o West DDC com a nuvem:

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

Veja a seguir um exemplo de arquivo SiteMerging.yml usado no exemplo anterior.

```
  East:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"
```

```
  DeliveryGroupPrefix: "East_"
  GroupPolicyPrefix: "East_"
  HostConnectionPrefix: "East_"
  MachineCatalogPrefix: "East_"
  StoreFrontPrefix: "East_"
  TagPrefix: "East_"
  AdminScopeSuffix: "_east"
  AdminRoleSuffix: "_east"
  ApplicationAdminSuffix: "_east"
  ApplicationFolderSuffix: "_east"
  ApplicationGroupSuffix: "_east"
  ApplicationUserSuffix: "_east"
  DeliveryGroupSuffix: "_east"
  GroupPolicySuffix: "_east"
  HostConnectionSuffix: "_east"
  MachineCatalogSuffix: "_east"
  StoreFrontSuffix: "_east"
  TagSuffix: "_east"
West:
  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"
  AdminScopePrefix: "Western "
  AdminRolePrefix: "Western "
```

```
  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "

  AdminScopeSuffix: ""

  AdminRoleSuffix: ""

  ApplicationAdminSuffix: ""

  ApplicationFolderSuffix: ""

  ApplicationGroupSuffix: ""

  ApplicationUserSuffix: ""

  DeliveryGroupSuffix: ""

  GroupPolicySuffix: ""

  HostConnectionSuffix: ""

  MachineCatalogSuffix: ""
```

```
StoreFrontSuffix: ""

TagSuffix: ""
```

Se um método central de compartilhamento de arquivos não for usado e a importação, mesclagem ou adição for feita a partir dos DDCs separadamente, crie e replique o arquivo SiteMerging.yml em cada DDC que está sendo migrado para a nuvem. O local padrão é *%HOMEPATH%\Documents\Citrix\AutoConfig*. Você deve especificar o parâmetro `–SiteName` para selecionar os prefixos de site corretos.

Mesclagem de sites

A Citrix recomenda realizar as operações de nuvem em etapas e fazer uma revisão completa de cada resultado antes de realizar a próxima operação de nuvem. Por exemplo, ao mesclar três sites em um único site de nuvem:

1. Mescle o site inicial com a nuvem usando o valor de `SiteName` apropriado.
2. Analise os resultados na interface de gerenciamento Full Configuration.
3. Se os resultados estiverem incorretos, determine o problema e sua causa, corrija-o e execute novamente a mesclagem. Se necessário, remova os componentes da nuvem e comece do zero usando `Remove-CvadAcFromSite` para o componente e os membros selecionados. Se os resultados estiverem corretos, continue.
4. Se a mesclagem inicial estiver correta, mescle o segundo site com o único site de nuvem.
5. Repita as etapas 2 e 3.
6. Se a segunda mesclagem estiver correta, mescle o terceiro site com o único site de nuvem.
7. Repita as etapas 2 e 3.
8. Revise os recursos da perspectiva do usuário e verifique se a exibição está no estado desejado.

Remover um componente usando o prefixo do site

Você pode remover seletivamente componentes de site único usando o prefixo no parâmetro `–IncludeByName` do cmdlet `Remove-CvadAcFromSite`. No exemplo a seguir, os grupos de entrega do West DDC não estão corretos. Para remover os grupos de entrega apenas para o site West:

```
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”
```

Para remover todos os componentes West, execute os seguintes cmdlets em ordem.

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName “Western *”
```

```
Remove-CvadAcFromSite –Applications –IncludeByName “Western *”
```

```
Remove-CvadAcFromSite – ApplicationGroups –IncludeByName “Western *”
```

```
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”
```

```
Remove-CvadAcFromSite –MachineCatalogs –IncludeByName “Western *”
```

```
Remove-CvadAcFromSite –HostConnections –IncludeByName “Western *”
```

```
Remove-CvadAcFromSite –Tags –IncludeByName “Western *”
```

Para remover as políticas de grupo dos componentes East, use o sufixo:

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName “*_east”
```

Histórico de documentos do Citrix DaaS

A tabela a seguir descreve alterações importantes na documentação do produto Citrix DaaS (antigo serviço Citrix Virtual Apps and Desktops). Essas alterações podem ser adicionais aos itens em Quais as novas.

Para o histórico do documento até novembro de 2024, consulte Histórico do documento anterior a dezembro de 2024.

Para receber notificações sobre essas atualizações, assine o feed RSS.

DATA	MUDAR	TÍTULO	DESCRIÇÃO
28 Feb 2025	Característica	**Suporte para provisionamento de disco de dados no Azure**	Agora você pode criar e atribuir um disco de dados persistente a uma VM persistente ou não persistente criada pelo MCS de um catálogo de máquinas MCS no Azure. O disco de dados é usado para armazenamento de dados persistentes, como logs de eventos, rastreamentos de segurança e dados de aplicativos. Saiba mais
27 Feb 2025	Característica	**Navegue facilmente do Studio para o Monitor para máquinas e sessões.**	Uma nova opção, **Exibir no Monitor**, agora está disponível no **Studio > Pesquisar**,

DATA	MUDAR	TÍTULO	DESCRIÇÃO
			fornecendo acesso mais rápido a informações detalhadas da sessão e da máquina no **Monitor**. Saiba mais
26 Feb 2025	Atualizar	**Economia de custos por meio da otimização do uso do armazenamento**	A página **Economia de custos** é aprimorada com visibilidade sobre a quantidade de economia obtida por meio da otimização do armazenamento quando as máquinas são desligadas. Saiba Mais
25 Feb 2025	Característica	**NitroTPM e inicialização segura UEFI para instâncias de VM AWS criadas pelo MCS**	Em ambientes AWS, agora você pode selecionar uma imagem mestre (AMI) habilitada com inicialização segura NitroTPM e/ou UEFI. Essa implementação garante que as VMs sejam seguras e confiáveis. Saiba mais
25 Feb 2025	Atualizar	**Monitorar melhorias de ação**	Agora você pode usar uma barra de progresso para ações e suporte para limitar o escopo das ações com base nas funções do usuário. Saiba mais

DATA	MUDAR	TÍTULO	DESCRIÇÃO
24 Feb 2025	Atualizar	**Limites**	Atualizados os limites do número de VDAs e grupos de aplicativos. Saiba mais
20 Feb 2025	Atualizar	**URLs na lista de permissões**	URLs da lista de permissões do Remote PowerShell SDK atualizadas. Saiba mais
18 Feb 2025	Atualizar	**Opção para visualizar e solucionar problemas de Sessões de Acesso Privado Seguro para implantações híbridas.**	Esse aprimoramento permite que clientes do DaaS que usam o Gateway, o StoreFront e o Secure Private Access no local monitorem e solucionem problemas de dados de sessão diretamente no DaaS Monitor. Saiba mais.
11 Feb 2025	Característica	**Compartilhe versões de imagens preparadas entre unidades de hospedagem no VMware**	Agora você pode usar o nó **Images** para compartilhar versões de imagens entre unidades de hospedagem dentro da mesma conexão de hospedagem no VMware. Você também pode usar comandos do PowerShell para atingir esse objetivo. Saiba mais

DATA	MUDAR	TÍTULO	DESCRIÇÃO
05 Feb 2025	Característica	**Suporte para criação de catálogos de máquinas MCS habilitados para MCSIO na AWS**	. Agora você pode criar catálogos MCS habilitados para MCSIO para criar catálogos de máquinas MCS habilitados para MCSIO na AWS para melhorar o IOPS de gravação direcionando as operações de gravação para o cache de write-back e para reduzir o tempo de inicialização quando o disco do sistema operacional persistente estiver habilitado. Saiba mais
30 Jan 2025	Característica	**Integração com Webhook**	O Citrix Monitor agora se integra ao Webhook, permitindo que você crie perfis de webhook para ferramentas como Slack, Microsoft Teams e ServiceNow na seção **Alertas e ITSM** na página **Integrações e exportações de dados** . Saiba mais.
24 Jan 2025	Atualizar	**Inicialização segura e vTPM**	Atualizamos o artigo para enfatizar que o vTPM não é um requisito para a

DATA	MUDAR	TÍTULO	DESCRIÇÃO
			Inicialização Segura e adicionamos conteúdo para o XenServer. Saiba Mais
22 Jan 2025	Característica	**Filtrar imagens mestras com base nas regiões da unidade de hospedagem**	Durante a criação do catálogo de computadores para a plataforma do Azure, o Studio agora pode filtrar e excluir imagens mestras que pertencem a regiões diferentes da região da unidade de hospedagem. Isso garante que apenas imagens da mesma região da unidade de hospedagem estejam disponíveis para seleção. Saiba Mais.
21 Jan 2025	Característica	**Adicionar aplicativos a implantações existentes da AWS no nó de implantação rápida**	Agora você pode adicionar aplicativos a implantações existentes da AWS, simplificando assim o processo geral de implantação. Saiba Mais.
21 Jan 2025	Característica	**Opção para redefinir contas do Active Directory (AD) em uso**	Com o Studio, agora você pode redefinir as contas do Active Directory (AD) da máquina, mesmo quando o status da máquina é Em uso.

DATA	MUDAR	TÍTULO	DESCRIÇÃO
21 Jan 2025	Característica	**Alertar os administradores de que as políticas de energia permanecem eficazes ao desabilitar o dimensionamento automático**	O aprimoramento serve para lembrar aos administradores que desabilitar o dimensionamento automático não afeta as configurações de política de energia para um grupo de entrega. Isso garante que os administradores estejam cientes do escopo da desativação do Autoscale e esclarece que as políticas de energia permanecem efetivas quando o Autoscale é desativado.
20 Jan 2025	Característica	**MCSIO com apenas cache de disco não é mais suportado**	A opção de configurar o MCSIO apenas com cache de disco (sem cache de memória) foi removida em todos os ambientes de hipervisor e serviço de nuvem. Saiba Mais
20 Jan 2025	Característica	**A criação de VMs da AWS usando propriedades de modelo de máquina não é mais compatível**	O **Aplicar propriedades de modelo de máquina a máquinas virtuais** foi removida da opção **Modelo de máquina** página. Em

DATA	MUDAR	TÍTULO	DESCRIÇÃO
			vez disso, crie VMs da AWS usando perfis de máquina para uma experiência semelhante e mais simplificada. Saiba Mais
20 Jan 2025	Característica	**Criar catálogo habilitado para MCSIO na AWS**	Com esse recurso, você pode criar um catálogo não persistente habilitado para MCSIO na AWS usando comandos do PowerShell. O MCSIO melhora o desempenho da VM armazenando em cache as operações de disco na memória ou em um disco pequeno e de alta velocidade. A opção de configurar o MCSIO apenas com cache de disco (sem cache de memória) usando o Studio foi removida em todos os hipervisores e ambientes de serviço de nuvem. Saiba Mais
17 Jan 2025	Característica	**Relatório de apps publicados menos usados e não usados**	Com esse recurso, você pode visualizar informações detalhadas de uso de aplicativos publicados

DATA	MUDAR	TÍTULO	DESCRIÇÃO
			acessados por meio do aplicativo Citrix Workspace, que ajuda a otimizar o gerenciamento de aplicativos e a alocação de recursos. Saiba Mais
16 Jan 2025	Característica	**Integração do Secure Private Access com o Monitor (versão prévia)**	Com esse recurso, você pode monitorar e solucionar problemas de todas as sessões de Acesso Privado Seguro no Monitor. Saiba Mais
15 Jan 2025	Atualizar	Local Host Cache	Atualizou todo o artigo para melhorar a precisão. Saiba Mais
26 Dec 2024	Atualizar	Remoção da tag de visualização da página Resumo de custos	Removida a tag Preview da tag **Economia de custos** recurso, pois o recurso foi lançado para disponibilidade geral. Saiba Mais
24 Dec 2024	Característica	**Cmdlets da ferramenta de configuração automatizada para backup e restauração**	Com esse recurso, você pode usar comandos do PowerShell compatíveis com a ferramenta de configuração automatizada para disparar as APIs de backup e

DATA	MUDAR	TÍTULO	DESCRIÇÃO
			restauração que o Studio usa. Saiba Mais
20 Dec 2024	Atualizar	Considerações sobre a instalação	Removida a referência a CTX139030 e redirecionada para Requisitos do sistema
16 Dec 2024	Característica	**Otimize o balanceamento de carga de armazenamento com o método de carga mínima**	Com esse aprimoramento, o Studio introduziu o **Otimize o balanceamento de carga de armazenamento com o método de carga mínima** opção. Se você selecionar dois ou mais locais de armazenamento de dados do sistema operacional durante a criação do catálogo, essa opção ficará disponível, permitindo que os discos sejam alocados para o repositório de armazenamento menos carregado. Saiba Mais
13 Dec 2024	Característica	**Guia Acesso privado seguro no Monitor**	Com esse recurso, o Citrix Monitor fornece um local dedicado para todos

DATA	MUDAR	TÍTULO	DESCRIÇÃO
			os novos recursos relacionados ao Secure Private Access. Saiba mais
13 Dec 2024	Característica	**Visibilidade para o serviço Secure Private Access**	Com esse recurso, o Citrix Monitor fornece monitoramento e visibilidade detalhados para aplicativos e usuários do Secure Private Access. Saiba mais#visibilidade-para-serviço-de-acesso-privado-seguro
13 Dec 2024	Característica	**Experiência de plataforma unificada para o Citrix Monitor**	Com esse recurso, o Citrix Monitor agora se alinha com todos os outros componentes do Citrix Cloud, fornecendo uma experiência de plataforma unificada. Saiba Mais
13 Dec 2024	Característica	**Aprimoramento da guia Conexões**	Com esse aprimoramento, o **Conexões** no Citrix Monitor agora oferece navegação simplificada para solução de problemas mais rápida. Saiba Mais

DATA	MUDAR	TÍTULO	DESCRIÇÃO
13 Dec 2024	Característica	**Filtrar detalhes do local do recurso**	Com esse recurso, o Citrix Monitor permite que você visualize o local do recurso para máquinas com sistema operacional de sessão única ou várias sessões no **Filtros** > **Máquinas** guia. Saiba Mais
13 Dec 2024	Característica	**Aprimoramento na guia Desempenho da sessão**	Com esse recurso, você pode usar o **Desempenho da sessão** no Citrix Monitor para monitorar métricas de endpoint adicionais que existem no aplicativo Citrix Workspace para Windows, Mac, Linux, HTML5 ou Chrome. Saiba Mais
13 Dec 2024	Característica	**Uso ativo da rede da máquina**	Com esse recurso, você pode usar o **Redimensionamento da carga de trabalho** no Citrix Monitor para obter informações detalhadas sobre o uso ativo da rede da máquina. Saiba Mais
13 Dec 2024	Característica	**Monitoramento de integridade do Cloud Connector**	Com esse recurso, você pode monitorar a integridade dos Cloud Connectors

DATA	MUDAR	TÍTULO	DESCRIÇÃO
			usando uma única exibição de painel e configurar alertas de forma proativa. Saiba Mais
10 Dec 2024	Característica	**SKUs somente NVMe**	Com esse recurso, o MCS dá suporte ao tipo de controlador de armazenamento NVMe para os novos SKUs de VM no Azure. Você pode criar um catálogo de máquinas MCS usando uma oferta de serviço que ofereça suporte apenas a NVMe ou SCSI e NVMe. Saiba Mais
10 Dec 2024	Característica	**Definir um fuso horário padrão para seu site**	Com o Studio, agora você pode definir um fuso horário padrão para o seu site Citrix DaaS. O Studio usa esse fuso horário para todas as exibições de horário e agendamento, como reinicialização agendada e dimensionamento automático. Saiba Mais
10 Dec 2024	Característica	**O Studio adota a navegação unificada do Citrix Cloud**	Como parte da mudança para uma experiência de navegação unificada

DATA	MUDAR	TÍTULO	DESCRIÇÃO
			em toda a plataforma Citrix Cloud, atualizamos o Studio para nos alinharmos a essa iniciativa em toda a plataforma. Saiba Mais
06 Dec 2024	Característica	**Provisionamento sob demanda da AWS**	Com o provisionamento sob demanda da AWS, o disco do sistema operacional é excluído quando você desliga uma VM não persistente. Essa implementação economiza custos quando a VM não está em uso. Saiba Mais
03 Dec 2024	Característica	**Mostrar configurações padrão seguras**	Esse recurso mostra a configuração padrão segura junto com a configuração padrão de uma política. A configuração padrão pode ser substituída pela configuração padrão segura. Saiba Mais